HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Herr
Benjamin Hartmann

Realisierung einer Mikrosegmentierung in einer „Software Defined“ Netzwerkumgebung zur Absicherung kritischer Infrastrukturen

2017

Fakultät **Angewandte Computer- und Biowissenschaften**

BACHELORARBEIT

Realisierung einer Mikrosegmentierung in einer „Software Defined“ Netzwerkumgebung zur Absicherung kritischer Infrastrukturen

Autor:
Benjamin Hartmann

Studiengang:
Angewandte Informatik - IT-Sicherheit

Seminargruppe:
IF13Wi-B

Erstprüfer:
Prof. Dr. rer. nat. Christian Hummert

Zweitprüfer:
Dipl.-Ing. (FH) Lars Huttenlauch

Mittweida, 2017

Bibliografische Angaben

Hartmann, Benjamin: Realisierung einer Mikrosegmentierung in einer „Software Defined“ Netzwerkumgebung zur Absicherung kritischer Infrastrukturen, 77 Seiten, 18 Abbildungen, Hochschule Mittweida, University of Applied Sciences, Fakultät Angewandte Computer- und Biowissenschaften

Bachelorarbeit, 2017

Referat

In dieser Thesis wird das Konzept des Software Defined Networkings (SDN) und den daraus resultierenden Möglichkeiten näher betrachtet. Auf dieser Grundlage wird beschrieben wie mit Hilfe einer SDN Umgebung eine kritische Infrastruktur abgesichert werden kann. Hierzu wird eine Mikrosegmentierung mit VMware NSX und auf Basis des VXLAN Protokoll realisiert. In weiterer Ausbaustufe werden zwei Rechenzentren zu einer hybriden Cloud zusammengeschlossen und demonstriert wie Layer 2 Datenverkehr zwischen beiden Rechenzentren transparent übertragen und dadurch die Sicherheit für solch ein Szenario erhöht wird. Darauf folgt ein Vergleich mit einer vergleichbaren Netzwerkumgebung, mit abschließender Beurteilung des Sicherheitsniveaus der implementierten Infrastruktur.

The following document describes the concept of Software Defined Networking (SDN) and its opportunities. Reasons will be shown, why it could be interesting and useful to implement a SDN to secure a business environment. The document also documentates an implementation of a SDN environment with VMware NSX and of a VXLAN. To bring the advantages of a SDN environment closer to the reader, the document describes how to realize a microsegmentation and strechting VXLAN over two different datacenters to make Layer 2 traffic transparent to protect critical infrastructures. At the end the author compares the installed SDN environment with a different SDN infrastructure and figures out the security level of a stand alone implementation of VMware NSX by using a microsegmentation.

I. Inhaltsverzeichnis

II. Abbildungsverzeichnis

III. Tabellenverzeichnis

IV. Abkürzungsverzeichnis

ACL ..... Access Control Lists
API ..... Application Programming Interface
ARP ..... Address Resolution Protocol
BGP ..... Border Gateway Protocol
CCDC ..... Cyber Capability Development Centre
CCDC ..... Cyber Capability Development Centre
CLI ..... Command Line Interface
DAN ..... Data Acquisition Network
DFW ..... Distributed Firewall
DHCP ..... Dynamic Host Configuration Protocol
DLR ..... Distributed Logical Router
DMZ ..... Demilitarisierte Zone
DND ..... Department of National Defence
DNS ..... Domain Name System
DRDC ..... Defense Research and Development
ECMP ..... Equal-Cost-Multi-path
FW ..... Firewall
Iaas ..... Infrastructure as a Service
IANA ..... Internet Assigned Numbers Authority
IEEE ..... Institute of Electrical and Electronics Engineers
IGMP ..... Internet Group Management Protocol
IP ..... Internet Protocol
IT ..... Informationstechnologie
LACP ..... Link Aggregation Control Protocol
LAN ..... Local Area Network
MAC ..... Media Access Control
MCAP ..... microcore and permiter
MPLS ..... Multi-Protocol Label Switching
MTEP ..... Multicast Tunneling Endpoint
MTU ..... Maximum Transfer Unit
NAP ..... Network Access Protection
NAT ..... Network Address Translation

NAV ..... network analysis and visibility
ONF ..... Open Networking Foundation
OSI ..... Open Systems Interconnection Model
OSPF ..... Open Shortest Path First
OTV ..... Overlay Transport Virtualization
Paas ..... Plattform as a Service
PIM ..... Protocol Independent Multicast
REST ..... Representational state transfer
RFC ..... Request for comments
SaaS ..... Software as a Service
SDC ..... Software Defined Computing
SDDC ..... Software Defined Datacenter
SDN ..... Software Defined Networking
SDS ..... Software Defined Storage
SG ..... Segmentation Gateway
SNMP ..... Simple Network Management Protocol
TCP ..... Transmission Control Protocol
ToR ..... Top of Rack Switches
UDP ..... User Datagramm Protocol
UTEP ..... Unicast Tunneling Endpoint
VDI ..... Virtual Deskto Infrastructure
VDS ..... vSphere Distributed Switch
VIB ..... VMware Installation Bundles
VLAN ..... Virtual Local Areas Network
VM ..... Virtuelle Maschine
vmdk ..... Virtual Machine Disk
VNI ..... VXLAN Netzwerk Identifier
VPN ..... Virtual Private Network
vSAN ..... Virtual Storage Area Network
VTEP ..... VXLAN Tunnel Endpoints
VXLAN ..... Virtual Extensible Lan
WAN ..... Wide Are Network
ZTNA ..... Zero Trust Network Architecture

1 Einleitung

Die Informationstechnologie (IT) und das Internet haben sich zu einem elementaren Bestandteil des Alltags entwickelt. Nicht nur Unternehmen sind auf die Technologie angewiesen, auch das Privatleben wird davon geprägt. Allein im Jahre 2016 gab es in Deutschland 58 Millionen Internetbenutzer [12]. Das Internet bildet eine weltweite Vernetzung unterschiedlicher Systeme, welche dessen Benutzern eine Vielzahl an Diensten offeriert. Angefangen von klassischen eMail Diensten bis hinzu der Bereitstellung von Anwendungen, welche über das Netzwerk ausgeführt werden und dadurch an jedem beliebigen Standort mit Internetanbindung genutzt werden können. Dies hat zur Folge, dass eine große Abhängigkeit von diesen Diensten besteht. Die Abhängigkeiten lassen sich in drei Kategorien zusammenfassen, organisatorische, wirtschaftliche und psychologische.

Organisatorische Abhängigkeit:
Das mobile Arbeiten mit Online-Diensten bedeutet, dass die Nutzer dieser Dienste auf Online Ressourcen zugreifen und diese aktualisieren können. Auf das Selbstverständnis, dass die Dienste im Zugriff sind, wurden private und geschäftliche Abläufe optimiert bzw. abgestimmt. Digitale Kalender werden beispielsweise über verschiedene Geräte aktualisiert und synchronisiert. Steht der Dienst oder eine Anbindung nicht mehr zur Verfügung, können die Datenbestände eine Inkonsistenz aufweisen, wodurch evtl. Abläufe eingeschränkt oder verzögert werden.
Viele Privatpersonen haben sich daran gewöhnt Ihr gesellschaftliches Leben mit Hilfe von Online-Diensten (Kalendern, Messenger) zu organisieren oder mit Hilfe von sozialer Medien mit anderen Menschen in Kontakt zu treten oder bestehende Kontakte zu pflegen.

Wirtschaftliche Abhängigkeit:
Für den Fortbestand eines Unternehmens oder einer Institution ist es unter Umständen existentiell, dass eine Internetverbindung oder Anbindung zu einem Außenstandort/ Hauptzentrale besteht. Die Anbindung der unterschiedlichen Standorte kann durch unterschiedlichste Technologien, wie Virtual Private Network (VPN) oder Multi-Protocol Label Switching (MPLS) hergestellt werden. Ist die Anbindung gestört, können Produktionen, Bestellvorgänge oder weitere betriebliche Prozesse stark eingeschränkt oder überhaupt nicht mehr durchgeführt werden. Hinzu kommt, dass viele Unternehmen mittlerweile planen Cloud-Dienste einzusetzen oder schon einsetzen. Cloud-Dienste können unterschiedlichste Formen annehmen. Diese beginnen beispielsweise bei dem Betreiben von Webseiten, eMail Diensten oder der Datenspeicherung. Diese Enterprise Produkte bieten Unternehmen eine höhere Flexibilität und kosteneffizienten Einsatz von Ressourcen. Die so genannten „. . . as a Service“ Produkte gibt es in den unterschiedlichsten Ausprägungen, wie:

- Infrastructure as a Service (IaaS):
  Es werden Rechenressourcen, wie Speicherplatz, Arbeitsspeicher, Prozessorleistung und Netzwerkressourcen zur Verfügung gestellt [7].
- Plattform as a Service (PaaS):
  Ist vor allem im Umfeld der Webanwendungen eingesetzt, da zu den aus dem IaaS genannten Funktionen noch eine Entwicklungsplattform und Tools zur Bereitstellung und Analyse zur Verfügung stehen. [8]
- Software as a Service (SaaS):
  Das Bereitstellen von Anwendungen, oder heute auch Apps genannt, über das Netz wird als Software as a Service tituliert. Hierbei wird die Hardware und Softwareumgebung vom Anbieter verwaltet und der Anwender kann sofort auf die Anwendungen zugreifen. [9]

Gründe für die Nutzung dieser Dienste liegen in der schnelle Verfügbarkeit, der nach Bedarf gerechten Skalierung, der Reduzierung des administrativen Aufwandes und der globalen Bereitstellung. Viele Aspekte einer leistungsfähigen Bereitstellung eines Dienstes oder Anwendung werden von dem Anbieten abgedeckt. Dies beginnt bei der Anbindung der Rechenzentren und deren internen Serversystemen, sowie Netzwerkkomponenten und endet bei der leistungsoptimierten Konfiguration der anzubietenden Dienste. Unter Umständen sind nicht nur Unternehmen wirtschaftlich von dem Internet abhängig. Viele Privatpersonen nutzen Dienste, bei welchen Sie entweder nicht mehr benötigte Gegenstände über Online-Auktionen verkaufen oder Online-Dienstleistungen als Kunde eines Unternehmens nutzen und hierdurch finanzielle Einsparungen erzielen, wie z.B. durch das Online-Banking.

Psychologische Abhängigkeit:
Aus den zuvor genannten Abhängigkeiten entsteht eine psychologische Abhängigkeit von Kommunikationsdiensten. Dies wird auf privater Ebene, sowie auf arbeitstechnischer Ebene ersichtlich. Ausfälle von Messenger Diensten lösen Empörungen und Schlagzeilen aus. Es entsteht das Gefühl ständig erreichbar sein zu müssen bzw. wird dies häufig von der Gegenseite erwartet. Dies wird aus einer repräsentativen Umfrage der Forsa im Auftrag von „RTL Aktuell“ vom 07. Mai 2017 ersichtlich. Dabei gaben 47% der Smartphone Nutzer an, dass „das Smartphone hingegen nicht mehr aus dem Alltag wegzudenken ist“. [5] Diese Abhängigkeiten führen dazu das von den Anbietern verlangt und erwartet wird, dass ihre Dienste an 24 Stunden, 7 Tage die Woche sicher, schnell und zuverlässig bereitgestellt werden. Bei Einschränkungen oder Ausfall einer der drei Kriterien kann es dazu führen, dass ein Dienst nicht mehr regelmäßig genutzt wird oder gar ganz vermieden wird. Die Folgen könnten materieller und/oder nicht materieller Art sein.

Jedoch sind nicht nur die Abhängigkeiten ausschlaggebend für die hohe Erwartungshaltung an die IT Umgebung. Es wird ein hohes Maß an Flexibilität gefordert. Möglichkeiten und wirtschaftliche Interessen erwarten eine schnelle Bereitstellung von Diens-

ten. Mit der Virtualisierung von Computersystemen ist diese Erwartungshaltung weiter gestiegen, Serversysteme können aufgrund von Vorlagen in Minuten ausgerollt und die darauf benötigten Anwendungen schnell installiert werden. Die Virtualisierung von Rechenleistung und Datenspeicher wird häufig als Software Defined Computing, bzw. Software Defined Storage zusammengefasst. Eine weitere Grundlage für die Kommunikation zwischen Server und Endgerät des Benutzers sind Netzwerke. Hierbei ist seit langem das Ethernet mit Transmission Control Protocol/Internet Protocol (TCP/IP) der Übertragungs- und Adressierungsstandard. Netzwerke sind aufgrund der wachsenden Anzahl an Teilnehmern und Diensten komplexer, umfangreicher und stoßen zum Teil an Grenzen Ihrer technischen Möglichkeiten. Häufig davon betroffen sind Adressräume, welche für Kundenanforderungen oder für Dienstleister nicht mehr ausreichend sind. Das Bereitstellen neuer Dienste verzögert sich häufig anlässlich der komplexen Planung und Konfiguration von Netzwerken. Sie werden dadurch häufig zum Flaschenhals der Projektumsetzung, da es bei der Einrichtung eines Netzwerkes viele Punkte wie Anbindungen, Datenverkehr und vor allem Sicherheitseinstellungen zu beachten gilt.
Zur Erlangung einer höheren Flexibilität innerhalb des Netzwerksegments existieren mittlerweile Technologien, welche die Netzwerkebene in ebenfalls eine virtualisierte Welt abstrahiert. Der Begriff des Software Defined Networking (SDN) tituliert diese Technologie. Alle drei Komponenten des Software Defined Computing (SDC), Storage (SDS) und Networking (SDN) werden unter dem Begriff des Software Defined Datacenters (SDDC) vermarktet und zusammengefasst und suggerieren eine völlige abstrahierte IT Infrastruktur. Diese Arbeit betrachtet den Bereich des SDN und gibt einen Überblick über die Technik von Virtual Extensible Lan (VXLAN) und dessen Vorteile.

1.1 Motivation

Die Anforderungen an Netzwerke steigen durch das laufend wachsende Angebot an Dienstleistungen im IT Sektor. Hinsichtlich der steigenden Anforderungen und der technologischen Möglichkeiten der Virtualisierung werden Systeme immer schneller ausgerollt. Hierdurch steigt die Anzahl der zu vernetzenden Systeme und daher auch das Kommunikationsaufkommen. Diese Informationen müssen transportiert und verarbeitet werden. Doch welche Daten laufen eigentlich durch das Netzwerk? Welche Systeme kommunizieren untereinander? Welche Kommunikation ist eventuell unerwünscht bzw. notwendig? Ist das Netzwerk flexibel und skalierbar? Der Aufwand zur Beantwortung dieser Fragestellungen ist in klassischen Netzwerken nur mit einem hohen Aufwand zu bewältigen.

Die klassischen Ansätze zur Segmentierung und Mandantenfähigkeit mit Hilfe von virtuellen Netzwerken in großen Umgebungen ist bei vielen Betreibern bald nicht mehr ausreichend. Die Erweiterung des Software Defined Networking bietet Möglichkeiten oben genannte Fragestellungen einfacher und schneller anzugehen, wobei vorgemerkt die Komplexität hierdurch nicht geringer wird. Die daraus resultierenden Möglichkeiten,

bieten jedoch weitere Optionen, die bei den klassischen Ansätzen gewünscht, aber nicht umsetzbar sind.
Unter diesen Gesichtspunkten und den Anforderungen an zukunftsfähige IT Infrastrukturen ist eine nähere Betrachtung des Software Defined Networkings und dessen Eigenschaften unerlässlich.

1.2 Software Defined Networking

Um einen Überblick über den Bereich der Netzwerkvirtualisierung und des SDNs zu erhalten ist es wichtig diese beiden Begriffe separat zu betrachten. Unter die Netzwerkvirtualisierung werden ebenfalls Technologien wie VPN und Virtual Local Areas Network (VLANs) zusammengefasst. Sie ermöglichen eine isolierte Kommunikation zwischen zwei Netzwerkgeräte über ein oder mehrere physische Netzwerke, auf welchen sich mehrere isolierte Netzwerke befinden können. Die Steuerungseinheit liegt dabei auf jeder einzelnen Netzwerkkomponente und müssen individuell aktualisiert werden. [26]
Das SDN setzt ebenfalls bei diesem Ansatz an und möchte diesen jedoch noch erweitern und die eigentliche Komplexität eines Unternehmensnetzwerkes in die virtuelle Ebene abstrahieren.
Die Open Networking Foundation (ONF) definiert den Begriff der SDN daher wie folgt:
„The physical separation of the network control plane from the forwarding plane, and where a control plane controls several devices.“ [10]
Die Definition bedeutet so viel, dass die vielen dezentralen Steuerungseinheiten auf den einzelnen Geräten zentralisiert werden müssen und eine zentrale Instanz für die Steuerung der teilnehmenden Netzwerkkomponenten zuständig ist. Hieraus hat die ONF eine hierarchische Abbildung 1.1 abgeleitet, welche ein Modell einer SDN Umgebung darstellt. Aus dieser Abbildung wird auch ersichtlich, dass die Steuerungseinheit weitere Funktionalitäten bietet, wie eine Programmierschnittstelle. Das Kernelement eines SDN ist die Steuerungsebene (Controller Plane) aus der Datenübertragungsebene (Data Plane) auszulagern und diese in eine eigenständige Ebene zu verschieben. Durch die Auslagerung erhält ein Administrator den Vorteil, dass es nur noch eine kontrollierende Instanz gibt, welche die Pfade zu entsprechende Netzen kennt und daher auch nur an dieser Stelle gepflegt werden muss. Die einzelnen logischen Geräte werden daher nicht vom Administrator selbst konfiguriert, sondern erhalten von einem Controller diese Informationen. Aktualisierungen werden von den logischen Geräten direkt an den Controller weitergeben, so dass diese Informationen den anderen teilnehmenden Netzwerkgeräten weitergegeben werden können, wenn die entsprechenden Richtlinien hierzu existieren. Die Replizierung zwischen den logischen Geräten entfällt hierdurch und die Entscheidung der effektivsten Pfade obliegt beim Controller. [10]
Der Controller kann durch zusätzliche Applikationen beeinflusst werden, welche über das Application Programming Interface (API) die Informationen erhalten, verarbeiten und danach Ihre Entscheidung an den Controller weitergeben. Dieser dirigiert dann den Paketfluss. Die Netzwerkkomponente ist dabei die ausführende Kraft, welche Ihre In-

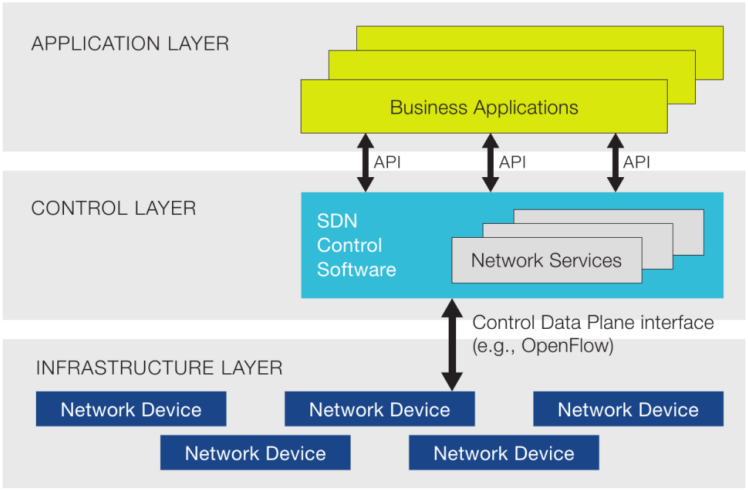

Abbildung 1.1: SDN Architektur [20]

formationen aus den lokal liegenden Informationen (Adresstabellen) entnimmt und das Datenpacket weiterleitet. Die lokalen Adressentabellen wurden zuvor von dem Controller aktualisiert. [10]

Auf diese Grundidee basierend definieren sich jedoch viele Hersteller den Begriff des SDN selbst um somit Ihre Ansichten des SDN in ihre Produkte einfließen zu lassen. Grundlegend können diese unterschiedlichen Auffassungen des SDN in drei unterschiedlichen Kategorien eingeteilt werden. [28, S.61]

- Open SDN
  SDN basierend nach Ansichten des ONF. Ein Controller aktualisiert Netzwerkkomponenten mit Hilfe des OpenFlow Protokolls, welches von den meisten Herstellern unterstützt wird.
- SDN via API
  Hierbei gibt es eine übergeordnete Software an welcher die Konfigurationseinstellungen hinterlegt werden und dann zentral ausgerollt werden können. Die einzelnen Netzwerkkomponenten bleiben dabei jedoch im eigentlichen Sinne selbständig. Die Steuerungsgewalt liegt immer noch auf den lokalen Netzwerkkomponenten.
- SDN via Overlay
  Beim Prinzip des Overlaying wird mit Hilfe einer Kapselung der Datenverkehr über ein Transportnetz an das Zielgerät gesendet.

Alle drei Kategorien besitzen jedoch die elementaren Bestandteile eines SDNs. [28, S.61-64]

1. Trennung der Daten- und Kontrollebene
2. Einfach gehaltene physische Netzwerkkomponenten, sie werden vom Controller

verwaltet.

3. Aufbauend auf Punkt zwei, gibt es eine zentrale Steuerungseinheit, den Controller.
4. Automation und Virtualisierung
   Es ist möglich ein virtuelles Netz anzulegen und dieses automatisiert zu administrieren, auszurollen, etc.
5. Systemoffenheit der Controller stellt eine API zur Verfügung, die transparent und dokumentiert ist. Es ist möglich über den Controller auf einzelne Schnittstellen (Netzwerkkomponenten) zuzugreifen.

Diese Arbeit setzt sich mit dem SDN via Overlays auseinander und beschreibt die genau Funktion in den folgenden Kapiteln, sowie die Umsetzung einer Testumgebung basierend auf VMware NSX.

1.2.1 SDN mit VXLAN

Eine sogenannte „overlay technology“ [44, S.18] ist das Virtual Extensible Local Area Network (VXLAN). Ein VXLAN Paket kapselte ein Ethernet Frame. Dies bedeutet, dass das ursprüngliche Ethernet Paket um zusätzliche Attribute erweitert wird. Diese Attribute oder auch Header genannt ermöglichen es Layer 2 (L2) Datenverkehr auf Basis von Layer 3 (L3) Netzwerken zu übertragen [33, S.7]. Hieraus entstehen mehrere Vorteile, welche das Verwalten und Erweitern von Netzwerken vereinfachen.

VXLAN Datenverkehr wird in einem User Datagram Protocol (UDP) Datenpaket übertragen. Die Internet Assigned Numbers Authority (IANA) hat VXLAN den Port 4789 zugewiesen [33, S.19]. Bei der Kapselung wird ein VXLAN Datenpaket um einen zusätzlichen Header mit einer eigenen Segmentkennung erweitert. Es können nur Geräte in einem Segment kommunizieren. Daraus folgt, dass der VXLAN Datenverkehr grundsätzlich voneinander isoliert ist. Der Datenverkehr wird erst zwischen zwei unterschiedlichen Segmenten sichtbar, wenn logische Instanzen installiert werden, welche die Verknüpfungen zwischen den einzelnen Segmenten herstellen. [44, S.74]

Eine weitere Eigenschaft von VXLAN ist, dass es unabhängig von dem Hersteller der physikalischen Netzwerkkomponente eingesetzt werden kann. Jedes Gerät, welches eine minimale Maximum Transfer Unit (MTU) von 1600 Bytes oder Jumbo Frames unterstützt, kann eine VXLAN Umgebung betreiben.
[33, S.9] Switche mit einer nativen VXLAN Unterstützung werden optional von einzelnen Herstellern angeboten, wodurch zusätzliche Funktionen bereitgestellt werden können, die das Übersetzen von VLAN in VXLAN oder vice versa unterstützen. Durch diese Funktion können L2 Netze (VLAN) über ein L3 Netz (IP) transportiert werden und in ein VXLAN Netz verbunden werden. Mit folgendem Praxisbeispiel soll dies veranschaulicht werden. Meistens findet eine Zuordnung zwischen VLAN und IP-Adressbereich

statt. Das Gleiche gilt auch bei einem Einsatz von VXLAN. Besteht nun ein physisches VLAN mit einem gültigen IP-Bereich, so ist es möglich eine Verbindung mit einem VXLAN herzustellen, welches den gleichen IP-Bereich anliegend wie das physische VLAN hat. Hierdurch können virtualisierte und physikalische Objekte auf L2 Basis miteinander verbunden werden. Dieser Vorgang nennt sich „Layer2 Bridging“. [44, S.47]

Nachfolgend werden kurz die einzelnen elementaren Bestandteile, bzw. Begrifflichkeiten einer VXLAN Umgebung erläutert:

- VXLAN Tunnel EndPoints (VTEP)
  VTEPs sind kapselnde oder entkapselnde VXLAN-Komponenten. Diese können z.B.: Virtualisierungsserver sein, auf welchen mehrere virtuelle Maschinen (VM) ausgeführt werden. Der von den virtuellen Maschinen getätigte Datenverkehr wird, wenn auf dem Virtualisierungsserver die VXLAN Funktionalität installiert ist, ge- und entkapselt. Damit ist der Virtualisierungsserver ein VTEP. Switche welche eine native VXLAN Unterstützung bieten und der Datenverkehr kapseln sind ebenfalls VTEPs. Komponenten welche keine aktive Kapselung betreiben und über die VXLAN Datenverkehr transportiert wird sind keine VTEPs. [3, S.3]
- VXLAN Network Identifier (VNI) / Segment Identifier (Segment ID)
  Kennung für ein VXLAN Netzwerksegment. Innerhalb eines Segmentes findet ein isolierter Datenverkehr statt. [33, S.10]
- Transportzone
  Der physikalische VXLAN Datenverkehr wird über ein physikalisches L3/L4 Netzwerk übermittelt. Erreicht wird dies durch die Anbindung einzelner VTEPs auf Basis des Internet Protokolls (IP) untereinander. Die Übertragung der Datenpakete erfolgt über das UDP Protokoll (L4). Aufgrund des klassischen Netzwerkaufbaus der Transportzone ist es möglich ein Segmentierungen von Transportzonen zu tätigen, um hierdurch ein optimiertes und isolierten Netzwerk innerhalb der Transportzonen aufzubauen. [44, S.104-105]

Aus der zuvor beschriebenen Funktionsweise von VXLAN geht hervor, dass VXLAN auch als Tunneling-Protokoll tituliert werden kann [33, S.7]. Es wird zwischen zwei Teilnehmern, den VTEPs, eine IPv4 oder IPv6 Konnektivität hergestellt und durch die entstandene Verbindung ist es für überliegende logische Instanzen möglich eine L2 Konnektivität herzustellen.

1.2.2 Aufbau eine VXLAN Pakets

Nachfolgend sollen die Attribute eines VXLAN Datenpakets von rechts nach links führend beschrieben werden. Bei der Auswahl handelt es sich um die wesentlichsten Merkmale, welche an dieser Stelle erläutert werden. [33, S.10-14]

- Original L2 Frame - max 1518 Bytes
  Das ursprüngliche Ethernet Datenpaket, welches von dem Endgerät innerhalb eines VXLANs gesendet wurde. Dieses Paket enthält auch die eigentlichen Informationen in seinem „Payload[1]“ - Bereich des Ethernet Paketes. Es findet keine Manipulation der Daten statt.
- VXLAN Header - 8 Bytes
  Erstes Erweiterungsattribut eines VXLAN Pakets

  – VNI VXLAN Network Identifier
    Der VNI kennzeichnet das Segment in welchem sich das Endgerät befindet. Die Kennung hat 24 Bit und daher knapp 16,8 Millionen Adressierungsmöglichkeiten.
- UDP Header - 8 Bytes
  Standard UDP Header

  – UDP Source Port
    Der Quellport wird mit Hilfe eines Hashwertes aus dem Orginal L2 Frame L2/L3/L4 Header errechnet. [44, S.19]
  – UDP Destination Port
    Wird auf den oben genannt VXLAN Port 4789 gesetzt.
- Outer IP Header - 20 Bytes
  Die Outer IP Adressen enthalten die IP Adressen der VTEPs

  – Outer Source IP
    IP Adresse des kapselnden Hostes
  – Outer Destination IP
    IP Adresse des zu entkapselnden Hosts, auf welchem sich das Zielgerät befindet.
- Outer Media Access Control (MAC) Header - 14 Bytes
  Abgeschlossen wird das VXLAN Datenpaket mit dem äußeren L2 Header.

  – Outer Source MAC Adresse
    MAC Adresse des absendenden VTEP Gerätes.
  – Outer Destination MAC Adresse
    MAC Adresse des zu empfangenden VTEP Gerätes.
  – VLAN Tag ID
    Optionale VLAN Kennung des Transportnetzes.

Aus der Abbildung 1.2 wird ersichtlich, wie das „Original L2 Frame“ um die zusätzlichen Attribute erweitert wird. Aufgrund dieser Erweiterung erhöht sich nun die Paketgröße auf 1568 Bytes.

[1] Als Payload wir der Nutzdatenbereich eines Paketes bezeichnet

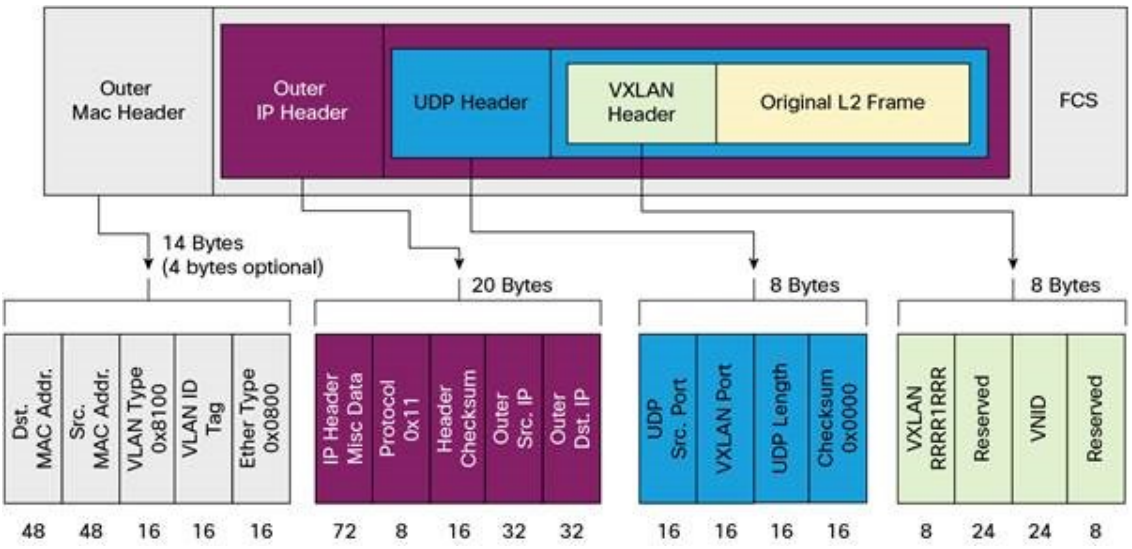

Abbildung 1.2: VXLAN Datenpaket [3, S.2]

$$
\begin{array}{rr}
 & 1518 \\
+ & 8 \\
+ & 8 \\
+ & 20 \\
+ & 14 \\
\hline
 & 1568
\end{array}
$$

1.2.3 Funktionsprinzip von VXLAN

Anhand eines schematischen Kommunikationsflusses von VXLAN sollen die theoretisch erlangten Informationen praxisnah beschrieben werden. Anschließend wird der Umgang mit „Multidestination-Traffic“ [44, S.35] dem Datenverkehr der von einem Endgerät an mehrere Endgeräte gesendet werden soll, beschrieben. Abschließend wird auf die Intentionen der Entwickler von VXLAN eingegangen.

In Abbildung 1.3 wird die Kapselung und Entkapselung eines VXLAN Pakets an zwei VTEPs dargestellt. Ziel innerhalb dieses Szenarios ist es, dass Host-A, welcher sich in dem VXLAN Segment 10 befindet, ein Datenpaket an Host-B, der ebenfalls Mitglied dieses Segmentes ist, erfolgreich versendet.
Der Host-A generiert nun ein Ethernet Frame, das „Original Frame “. Dieses enthält die Informationen und standardmäßigen Attribute/Header einer Ethernet Kommunikation. Diese wären der TCP/IP und MAC Header. Host-A gibt als Zieladresse die IP und MAC Adresse von Host-B an.
Das VTEP-1 nimmt das von Host-A gesendete Paket auf und überprüft anhand seiner lokal geführten Tabellen auf welchem VTEP sich Host-B befindet. VTEP-1 stellt anhand der Tabelle fest, dass sich Host-B auf VTEP-2 befindet. Aufgrund dieser Informationen ergänzt nun VTEP-1 das von Host-A gesendete Paket um die zusätzlichen Attribute.

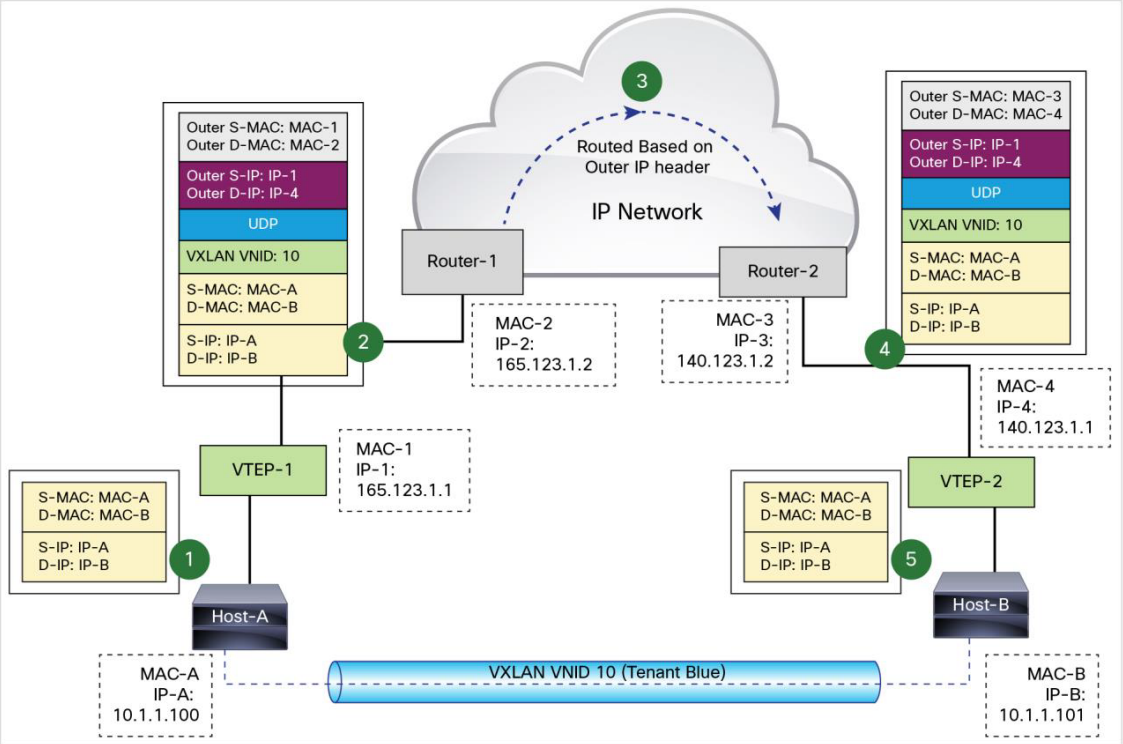

Abbildung 1.3: VXLAN Kapselung [3, S.4]

Zuerst wird die VNI/Segment ID hinzugefügt. Anschließend der Outer-IP Header, also die IP-Adresse von VTEP-1 als Quelladresse und als Zieladresse die von VTEP-2. Abgeschlossen wird das VXLAN Paket durch den Outer-MAC Header, welcher ebenfalls als Quelladresse die MAC von VTEP-1 und als Zieladresse die MAC von VTEP-2 enthält.
Da sich beide VTEPs in unterschiedlichen Netzwerksegmenten befinden, welche durch unterschiedliche IP Adressen gekennzeichnet sind, wird das Datenpaket aus dem VTEP-1 IP-Segment über Router-1, an Router-2 in das entsprechenden IP Segment von VTEP-2 weitergeleitet.
Das Paket wurde nun erfolgreich an VTEP-2 übermittelt. Dieser entkapselt nun die äußeren Attribute Outer-MAC, Outer-IP und VXLAN Header. Nach der Entkapselung wird das „Original Frame “ an den Host-B übermittelt. Host-B hat von den vorherigen Aktivitäten der Kapselung keine Kenntnis und interpretiert den ihm vorliegenden Datenverkehr innerhalb seines Netzwerksegmentes. [3, S.4]

Wie eingangs schon beschrieben findet VXLAN Datenverkehr von Grund auf isoliert statt. Dabei zu beachten gilt es, dass dies für den logischen Datenverkehr gilt. Innerhalb einer Transportzone werden alle entsprechende VXLAN Pakete über diese gesendet und sind daher ersichtlich und potenzielle Angriffsziele [33, S.18]. Teilnehmer der logischen Netze können jedoch nur den Verkehr einsehen, welcher sich in ihrem Segment befindet. Für sie ist es nicht ersichtlich, ob es sich um einen logischen oder physikalischen Anschluss handelt. Gewährleistet wird dies auch durch die VTEPs, wel-

che Pakete intelligent und zielgerichtet übermitteln. [44, S.74-75]
Das zuvor beschriebene Szenario bezieht sich auf einen 1:1 Datenverkehr, also von einem und zu einem Endgerät. Ein weiteres Szenario ist bekannt als „Multidestination-Traffic“. Hierbei möchte ein Endgerät gleichzeitig eine Mehrzahl an Endgeräten mit gleichen Datenpaketen versorgen. Es entsteht also eine 1:n Relation. Diese Art von Datenverkehr tritt auf bei:

- Broadcast
  Der Broadcast ist ein Rundruf an alle Mitglieder eines Netzwerksegmentes. Welcher eingesetzt wird um einen Überblick zu erhalten, welche Geräte sich in einem Netzwerksegment befinden. [31, S.3]
- unknown unicast
  Diese Form des Multidestinations-Traffic tritt auf, wenn ein Endgerät ein Datenpaket sendet und der Empfänger dem Switch nicht bekannt ist. Der entgegennehmende Switch leitet das Paket an alle Schnittstellen, an deren das Netzwerksegment anliegt weiter und hofft dabei, dass das Paket zugestellt wird. [21]
- Multicast
  Multicast Verbindungen treten häufig bei Multimedia Übertragungen auf. Das Ziel hierbei ist es einer bestimmten Gruppe von Systemen die gleichen Informationen bereitzustellen. Vergleichbar mit Broadcasts, wobei sich Multicasts nicht zwingend auf alle Mitglieder eines Segmentes beziehen bzw. Verbindung in andere Netzwerksegmente herstellen. Des Weiteren kann ein Multicast-Gruppen Mitglied selbst entscheiden ob er weiterhin Teil einer Gruppe ist oder nicht. [1, 32, S.1]

Aufgrund der Architektur kommt in einer VXLAN Infrastruktur viel Multidestination-Traffic vor. Auf die Behandlung dieses Datenverkehrsaufkommen wird in den nachfolgenden Kapiteln 1.2.4 und 2.1 eingegangen.
Bei einem Multicast-Konstrukt werden sogenannte Multicast-Gruppen gebildet. Multicasting wird meistens auf der dritten Ebene des Open Systems Interconnection Model (OSI) Referenzmodells angewendet. Hierfür sind von der IANA in dem Requests for Comments (RFC) 5771 IP Bereiche definiert worden. Die Einrichtung einer Multicastumgebung erfordert die Manipulation von Netzwerkkomponenten, da an diesen Stellen die Gruppenzugehörigkeit auf Basis des Internet Group Management Protocol (IGMP) hinterlegt werden müssen. Die Vorteile einer Multicast-Umgebung sollen am Beispiel (Abbildung 1.4) eine Address Resolution Protocol (ARP) Broadcasts beschrieben werden. [3, S.6]

1. ARP Anfrage nach der IP des Systems B wird End-System-A versendet
2. VTEP-1 registriert eine ARP Anfrage
   VTEP-1 durchsucht die lokale Adresstabellen ob IP-B bekannt ist. Wenn dies nicht der Fall ist kapselt VTEP-1 das Paket und sendet es an die Multicast Gruppe. In diesem Fall sind dies VTEP-2 und VTEP-3.

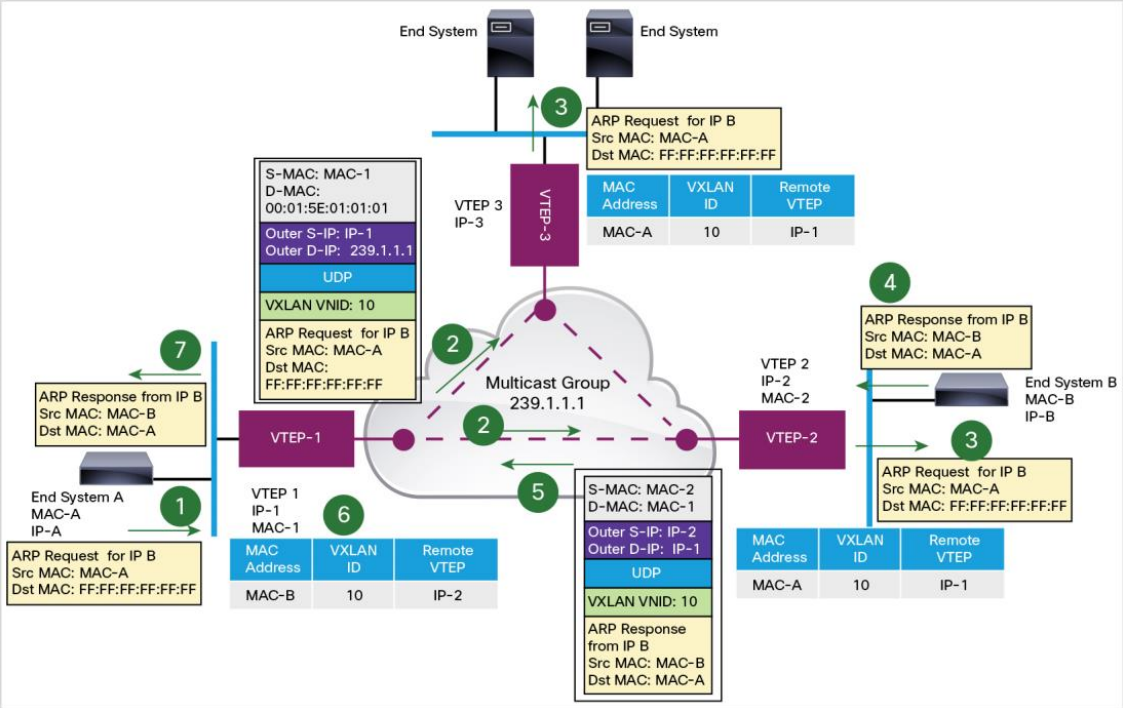

Abbildung 1.4: VXLAN Multicasting [3, S.6]

3. VTEP-2 und VTEP-3 empfangen ein Multicastpaket aufgrund der Mitgliedschaft VXLAN Paket wird entkapselt und die ARP Anfrage an alle Endsysteme des VXLAN Segmentes weitergeleitet. Zusätzlich hinterlegen alle VTEP System die IP von End-System-A ihre lokalen Tabellen, sollte dies noch nicht vorhanden sein.
4. End-System-B beantwortet ARP Anfrage
   End-System-B an VTEP-2 erhält ARP Anfrage, hinterlegt in seinem lokalen Speicher die IP zu MAC Zuordnung von End-System-A und beantwortet die Anfrage.
5. Rückantwort von End-System-B wird vom VTEP-2 entgegengenommen
   Das Paket mit der ARP Rückantwort von End-System-B wird in ein VXLAN Paket gekapselt und als Unicast an VTEP-1 gesendet. VTEP-2 ist durch die im Schritt 3 erhaltene Anfrage von End-System-A bekannt an welchem VTEP das Endgerät anliegt. Dadurch kann die Antwort zielgerichtet weitergeleitet werden.
6. VTEP-1 verarbeitet Rückantwort
   VTEP-1 empfängt das VXLAN-Paket und wird entkapselt. Erneut werden die Inhalte der lokalen Adresstabelle um die neuen Einträge des VTEPs erweitert. VTEP-1 hinterlegt, wenn noch nicht vorhanden, die IP des VTEP-2 und speichert die IP-MAC Zuordnung von End-System-B.

Durch das Verwenden von Multicast-Gruppen ist es möglich den Datenverkehr zu reduzieren. Ohne die Verwendung von Multicasts, müsste VTEP-1 die ARP Anfrage jeweils an VTEP-2 und VTEP-3 selbst versenden. Des Weiteren werden bei der Einteilung in Multicastgruppen nur die Teilnehmer informiert die es auch betreffen.
Aus diesem Betrachtungswinkel wird ersichtlich, dass die Entwicklung von VXLAN haupt-

sächlich unter dem Gesichtspunkt des Einsatzes in große Netzwerkumgebungen bestand. Große Infrastrukturen werden hauptsächlich bei Großunternehmen oder Rechenzentrumsbetreibern angetroffen. Häufige Problemstellungen mit welchen sich Betreiber solcher IT-Landschaften konfrontiert sehen: [33, S.6]

Erweiterung des beschränkten VLAN Adressraumes
Der Adressraum für VLAN Netzwerke beträgt lediglich $2^{12} = 4096$ wobei die unterste Adresse 0 und die oberste Adresse 4095 reserviert sind. Abhängig vom Hersteller einer Netzwerkkomponente können weitere VLAN Kennungen reserviert sein. Für Betreiber von Rechenzentren bei welchen eine isolierte Mandantenumgebung betrieben wird kann unter Umständen der verfügbare VLAN Adressraum nicht mehr ausreichend sein. Durch den zusätzlichen VXLAN Header steht in einer VXLAN betriebenen Umgebung ein $2^{24} = 16.777.216$ Layer 2 Adressraum zur Verfügung. [33, S.7]

Mandantenfähigkeit
Bei einer Mandantenfähigkeit wird die Erwartung an eine Umgebung gestellt, bei parallel betriebenen Umgebungen den Datenverkehr oder den Ressourcenzugriff so zu reglementieren, dass die verschiedenen Umgebungen isoliert und autark voneinander betrieben werden können. Ein Beispiel für Mandantenumgebungen sind Rechenzentrumsbetreiber, bei denen mehrere Kundenlandschaften parallel betrieben werden. [33, S.6]

Entlastung der Top of Rack Switches (ToR) Adressenverwaltung
Ein ToR ist ein Switch, welcher bildlich an oberster Stelle des Serverschrankes (Rack) platziert ist und an wessen alle Server dieses Schrankes angeschlossen sind. Die in dem Betriebssystem des Switches integrierte Adressentabelle musste vor dem Virtualisierungszeitalter je Port eine Media Access Control (MAC) Adresse kennenlernen und pflegen. Seit der Computervirtualisierung kommen noch zusätzliche Adressen hinzu. Die Adresse des Virtualisierungsserver (Hypervisor), sowie Adressen der virtuellen Maschinen, welche ebenfalls die Netzwerkschnittstelle des Hypervisor nutzen. Bei großen Infrastrukturen und vielen virtuellen Instanzen können Switche an die Grenze der zu verwaltenden Adressen gelangen, was sich auf die Leistung des Netzwerkes auswirken kann. [33, S.7]

1.2.4 Software Defined Networking mit VMware

Das folgende Kapitel vereint die beiden zuvor beschriebenen Unterkapitel „Software Defined Netwoking“ und „VXLAN “ und gibt auf Basis von VMware NSX einen Einblick in die Funktionsweise einer SDN Umgebung. Mit der Übernahme der Firma Nicira, einem SDN und Netzwerkvirtualisierungs Hersteller, im Jahre 2012, ist VMware in den Bereich des SDN vorgestoßen. [37, S.2]

Ohne eine zuvor grundlegende Einführung in die betreffenden VMware Produktwelt ist es nur schwer möglich die Funktionsweise von NSX zu erläutern. Deshalb soll an dieser Stelle eine kurze Beschreibung der eingesetzten Produkte in diesem Projekt und NSX Komponenten erfolgen.

VMware vSphere
VNware vSphere ist das Virtualisierungsprodukt für Computerressourcen und beinhaltet das Virtualisierungsbetriebssystem VMware ESXi. Nach der Installation des Betriebssystems und erfolgreicher Grundkonfiguration hat der Benutzer die Möglichkeit virtuelle Computerinstanzen auf dem Server, auch Hypervisor genannt, einzurichten und zu betreiben. Der Hypervisor abstrahiert die Hardware des physikalischen Servers und stellt dieser einer virtuellen Maschine bereit. Festplatten werden in Dateien abgebildet, den sogenannten vmdk Dateitypen. Damit virtuelle Maschinen auf Netzwerke zugreifen können muss der Hypervisor diese Ressource abstrahieren. Hierzu wird zwischen dem physikalischen Netzwerkadapter des Hypervisors ein vSphere Switch installiert. Ein vSphere Switch gibt es in zwei Ausführungen. Der „vSphere Standard-Switch “ steht lokal an einem ESXi Server zur Verfügung. Die zweite Variante ist der „vSphere Distributed-Switch“ (VDS) der zentral an mehrere ESXi Server ausgerollt werden kann. VDS haben in der VMware NSX Umgebung eine hohe Relevanz und sind die Grundlage für das Bereitstellen von virtuellen Netzwerken [44, S.112].

VMware vSphere vCenter
Das vCenter ist die zentrale Administrationsoberfläche für VMware Komponenten. Es ist die Grundlage zur Nutzung von erweiterten Funktionen, wie z.B. den Einsatz von VDS und das Clustern von Virtualisierungsservern. Des Weiteren können zusätzliche VMware Erweiterungen integriert werden und den Funktionsumfang nochmals vergrößern. NSX ist eine hiervon. [16]

VMware vSAN
Virtual Storage Area Network (vSAN) bietet innerhalb einer VMware Umgebung Datenspeicher von vSphere Servern zur Virtualisierung an. Bei der Virtualisierung von Datenspeicher mit vSAN werden einzelne lokale Festplatten eines Hypervisors, auch Knoten genannt, markiert und mit den anderen Festplatten anderer Knoten eines Clusters in einen virtuellen Datenspeicher zusammengefasst. Die Anbindung der Server sollte daher auch dementsprechend ausgelegt sein. Diese virtuelle Festplatte wird als ein neuer Datastore angelegt. Ein Cluster Verbund besteht aus Flashspeicherplatten und es können optional noch Kapazitätsplatten ausgewählt werden. Der Unterschied zwischen beiden Varianten ist: [27, S.5]

- Flashspeicher
  Der Flashspeicher dient als Kurzspeicher um die Leistung des Festplattensystems zu garantieren. [27, S.5]
- Kapazitätsplatten

Der Kapazitätsspeicher bildet den dauerhaften Speicher eines vSAN Systems. [27, S.5]

VMware NSX

Der letzte Baustein eines Software Defined Datacenters (SDDC) ist die Netzwerkvirtualisierung. Dieses wird bei VMware mit dem Produkt NSX angeboten. Aufgrund der Tatsache das NSX auf VXLAN basierend ist, haben Grundbegriffe wie VTEP, Transportzone, etc. weiterhin die zuvor beschriebene Bedeutung und Funktion. Zur leichteren Veranschaulichung wird das VMware NSX Konstrukt in drei Ebenen eingeteilt: Management-, Controller- und Datenebene.

Die Managementebene bildet die Administrationsoberfläche und das Application Programming Interface (API). Sie dient zur Konfiguration und Überwachung der NSX Infrastruktur. Die API ist auf Representational state transfer (REST) basierend und bietet Möglichkeiten zur Automation [44, S.6].
Die NSX Managementkomponenten beinhalten den NSX Manager und den vCenter Server. Ein NSX Manager steht in einer 1:1 Relation mit einem vCenter Server und stellt dabei die Konfigurationsoberfläche dar. Ebenfalls auf dieser Ebene angesiedelt ist die Integrationsmöglichkeit von Drittherstellern um Sicherheitsfunktionen zu erweitern. Die Managementebene ist von der Controller- und Datenebene autark. Bei einem Ausfall kann die Controll- und Datenebene weiter arbeiten. Einzelne Funktionalitäten welche auch die Controllerebene betreffen, wie die Restful API, stehen nicht zur Verfügung. [44, S.13-14]
Innerhalb der Controllerebene befinden sich die Netzwerksteuerungseinheiten. Controller dirigieren den Datenfluss innerhalb des logischen Netzwerkes. Nachfolgend eine kurzer Überblick über die Darstellung der einzelnen Komponenten. Aus der Beschreibung der Komponenten und deren Aufgaben soll auch das Zusammenspiel der einzelnen Komponenten aufgezeigt werden.

NSX Manager

Ist für die Verteilung von Richtlinien, IP-Adressen der NSX-Controller Knoten, Private Keys und Zertifikaten zur Kommunikation verantwortlich. Es werden auch grundlegende Einstellungen des NSX Managers wie vCenter-Synchronisation und Systemeinstellungen hinterlegt. Die Distributed Firewall Richtlinien werden hier bearbeitet und an die betreffenden Systeme verteilt. [44, S.13,28]

NSX Controller

Die NSX-Controller sind für das Replizieren der unterschiedlichen Adresstabellen zuständig. Die Adressentabellen enthalten eine VTEP-, MAC- und Routing-Tabellen [44, S.22]. Sie sind somit die Lenkzentrale. NSX-Controller werden in einem Cluster, mit einer ungeraden Anzahl von mindestens drei Knoten, bereitgestellt [44, S.11].

NSX Edge Services

Die NSX Edge Services bilden die Schnittstelle zwischen dden physikalischen und abstrakten Netzwerken. Innerhalb des Software Defined Networkings wird Datenverkehr, welcher zwischen diesen beiden Welten fließt wird „North-South Traffic“ genannt. Edge Services bieten zusätzliche Dienste wie Network Address Translation (NAT), Firewall. Load Balancing, VPN, Dynamic Host Control Protocol (DHCP) und Domain Name System (DNS). Eine weitere wichtige Funktion die den Edge Services zukommt ist die des Routings. Es werden dabei auch dynamische Routing Protokolle Open Shortest Path First (OSPF) und Border Gateway Protocol (BGP) unterstützt. Diese sind mit einer der Gründe weshalb Edge Services als virtuelle Maschinen auf einem Hypervisor ausgerollt werden müssen. Hierbei kommuniziert die virtuelle Maschine mit den Controllern um neu erlernte Routen mitzuteilen oder Routen zu löschen. [44, S.22-23]

Switche und Portgruppen

NSX benötigt für die Bereitstellung von logischen Netzen eine physische Übertragungsstrecke (Transportzone) welche an den Hypervisors angebunden ist. Mit Hilfe von VDS wird der physische Netzwerkadapter abstrahiert. Dies ist auch der Grund weshalb der VDS essentiell für die Betreibung von NSX Infrastrukturen ist. Der VDS stellt nun die Konnektivität zu den physischen Netzwerkadaptern des Hypervisors her. Die Vernetzung der unterschiedlichen Virtualisierungsserver auf diesen Adaptern bilden das Transportnetz. Wichtig hierbei zu beachten gilt, dass VMware mindestens eine MTU Größe von 1600 Bytes für das Transportnetz voraussetzt [44, S.24].
Die virtuellen Adapter von virtuellen Maschinen werden an Portgruppen gebunden. Bei den Portgruppen gibt es auch zwei Varianten, Standard oder Verteilte Portgruppen. Die Eigenschaften sind simultan zu denen von verteilten „vSphere Switchen “ und „Standard vSphere Switche“. Die Portgruppe wird an einen vSphere Switch gebunden. Somit ist der vSphere Switch und die Portgruppe das Abstraktionsmittel, wodurch die Verbindung zwischen virtueller und physischer Welt hergestellt wird. Bei der Erstellung eines neuen logischen Switches (vSwitch) wird auf dem VDS der Transportzone eine neue Portgruppe erstellt. Dieser Logische Switche ist eine Portgruppe an dem VDS und verbindet angeschlossene virtuelle Maschinen auf Layer2 Basis. Portgruppen sind isoliert voneinander, dies bedeutet VMs an unterschiedlichen Portgruppen anliegend können nicht miteinander kommunizieren. [46, S.78-79]

Distributed Logical Router

Distributed Logical Router (DLR) sind die virtuellen Router, welche unterschiedliche logische Switche miteinander verbinden können und somit eine Konnektivität auf Layer3 basierend innerhalb der virtuellen abstrakten Struktur herstellen können. Grundlegend sind DLR und Edge Systeme ähnlich, jedoch gibt es Unterschiede in der Anzahl an zu Verfügung stehenden Netzwerkadaptern und den möglichen Diensten. Des Weiteren ist es möglich DLR virtuell auszurollen, wodurch keinen VM des Routers instanziiert wird. Diese Form der DLRs besitzen eine Einschränkung, ein dynamisches Routing und Firewalling kann nur mit DLRs umgesetzt werden. wenn diese eine virtuelle Instanz ausgerollt haben. [44, S.52-56]

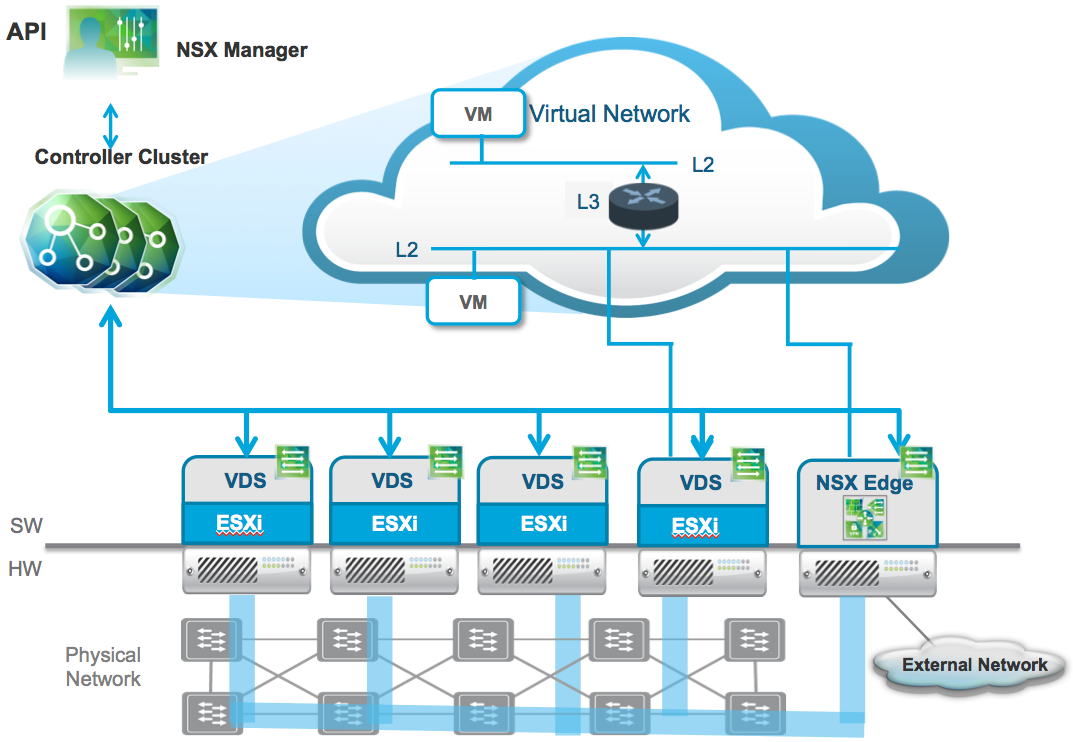

Abbildung 1.5: NSX Infrastruktur [44, S.8]

Die Virtualisierungsserver bilden in einer solchen Umgebung der VTEPs. Ihrer Netzwerkadapter sind mit dem VDS der Transportzone verbunden und bilden daher die „Outer MAC und IP Address Header“. Jeder logische Switch erhält eine ID, dabei handelt es sich um die VNI oder in VMware auch Segment ID genannt. Das von der virtuellen Maschine generierte Paket beinhaltet somit das „Original Frame“, also die „Nutzdaten“ und die Netzwerkinformationen des Netzes der VM. Wie bereits in Kapitel 1.2.3 erläutert ist Multidestination Traffic, auch „BUM Traffic “ genannt, innerhalb NSX ein wichtiger Faktor. Aus diesem Grund werden an dieser Stelle nochmals die verschieden Modi zur Replikation eines Multidestination Traffic innerhalb NSX dargestellt. BUM ist dabei die Abkürzung für Broadcast, unknown unicast und Multicast, welche schon zuvor in Kapitel 1.2.3 beschrieben worden sind. Die Komplexität innerhalb einer SDN Umgebung ist, dass Transportzonen sich über mehrere Netzwerksegmente erstrecken können. Dies bedeutet VTEP Geräte, auf welchen sich virtuelle Instanzen in einem logischen Netz befinden (gleiche VNI), besitzen unterschiedlichen Netzwerkadressen. Die Konnektivität der VTEPs wird durch Router- und Switchkomponenten sichergestellt. NSX besitzt drei Replikationsmodi zur Behandlung von Multidestination Traffic. Diese sollen anhand einer ARP Anfrage am Beispiel der Abbildung 5 gezeigt werden. ESXi1 und 2 bilden das Subnetz A der Transportzone und ESXi 3 und 4 das Subnetz B. VM1 bis VM4 befinden sich in diesem Beispiel in demselben logischen Netzwerk. Ausgehend von einer ARP Anfrage von VM1 soll diese an alle VMs gesendet werden. Der Prozess des Kapselns und Entkapseln der VTEPs wird hier nicht nochmal explizit erwähnt. [44, S.35-41]

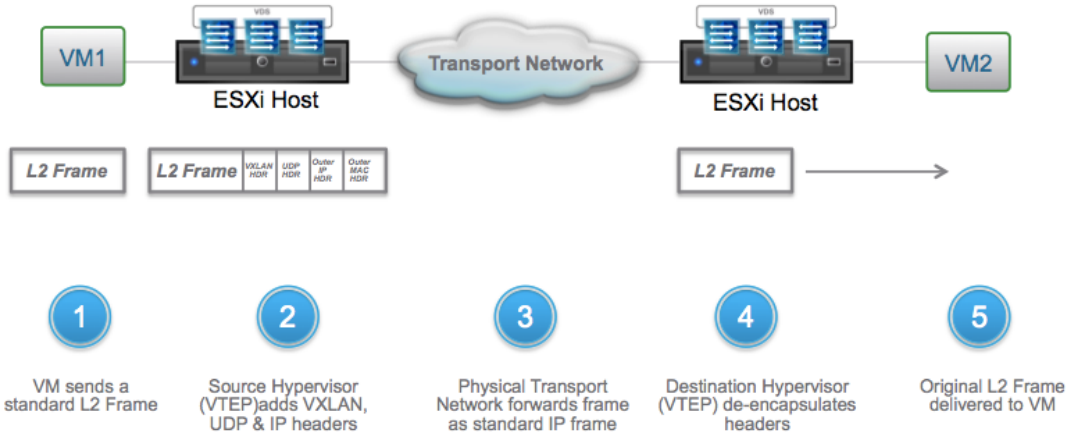

Abbildung 1.6: VTEP VXLAN-Kapselung [44, S.13]

- Unicast Mode
  Beim Unicast Mode sind keine Modifikationen an den Netzwerkkomponenten notwendig. In jedem Subnet gibt es einen Unicast Tunneling Endpoint (UTEP), welcher bei jeder Multidestination Transaktion zufällig neu bestimmt wird bzw. abweichend sein kann. Sendet VM1 eine ARP Anfrage wird diese von ESXi1 empfangen. ESXi1 weiß anhand der VTEP Tabelle welche Teilnehmer in diesem VXLAN vorhanden und an welchen VTEP sie anliegend sind. Aus diesem Grund wird das Paket an ESXi2 weitergeleitet. Im SubnetB besitzen ESXi3 und 4 ebenfalls Teilnehmer in diesem VXLAN. ESXi1 leitet daher die ARP Anfrage an ESXi3 weiter. ESXi3 wird zum UTEP und ist dafür zuständig, dass alle VTEPs welche ein Mitglied in diesem VXLAN von VM1 besitzen die ARP Anfrage erhalten. ESXi3 übermittelt deshalb das ARP Paket an ESXi4. [44, S.38-40]
- Multicast Mode
  Das Prinzip des Multicasts wurde im vorherigen Unterkapitel näher beleuchtet und unterscheidet sich unter VMware nicht. Bei der Verwendung des Multicast Replikationsmodus müssen mehrere Einstellungen an den Netzwerkkomponenten vorgenommen werden. An den jeweiligen Switches von Subnet A und B müssen die IGMP Gruppen zugeordnet werden und an den Routern muss das Protocol Independent Multicast (PIM) konfiguriert werden. Bei der Zuordnung der Multicastgruppen gilt: je detaillierter eine Zuordnung vorgenommen wird, desto höher ist der Konfigurationsaufwand und die Wartung. Findet eine zu grobe Einteilung statt ist das Datenaufkommen höher.
  VM1 sendet ein ARP Paket, dieses wird von ESXi als Multidestination Traffic erkannt. Bei der Verwendung von Multicast wird jedem logischen Netz ein Multicast IP Adressbereich zugewiesen. An die Multicastadresse wird das Paket versendet und erreicht den Switch des SubnetA. Der Switch erkennt an der IP Adresse das es sich um ein Multicast Übertragung handelt und sendet anhand der IGMP Zugehörigkeit das Paket an ESXi2 und an den Router, da sich in SubnetB ebenfalls Mitglieder dieser IGMP Gruppe befinden. Der Switch in Subnet B sendet an

alle VTEPs, ESXi 3 und 4, das ARP Paket. Angenommen VM4 wäre nicht im gleichen VXLAN, dann würde das ARP Paket nicht an ESXi4 weitergeleitet worden. [44, S.36-38]

- Hybrid Mode
  Der Hybrid Mode ist eine Kombination aus Unicast- und Multicast Mode. Dies bedeutet es sind teilweise Änderungen an den Netzwerkkomponenten vorzunehmen. Im Hybrid Mode wird ebenfalls auf IGMP gesetzt. Jedoch ist es nicht notwendig einen PIM Router einzusetzen. Für das Beispiel einer ARP Anfrage gilt dann, dass VM1 wieder eine ARP Anfrage generiert. Am Switch des SubnetA und SubnetB sind wieder IGMP Gruppen hinterlegt. ESXi1 fängt nun die ARP Anfrage ab und sendet eine Multicast Paket an den Switch des SubnetA. ESXi2 hat ebenfalls eine VM in diesem VXLAN und leitet daher das Paket an ESXi2, welches es an die VM2 weiterleitet. Anhand der VTEP Table, erkennt ESXi1, dass im SubnetB weitere Teilnehmer in diesem VXLAN existieren. ESXi1 erzeugt daher ein Unicast Paket, welches an ein VTEP im SubnetB gesendet wird. Dieses VTEP ist daraufhin auch ein Multicast Tunneling Endpoint (MTEP) für die Übertragung. Das MTEP, in diesem Fall ESXi3, leitet das Paket an VM3, welche auch in dem VXLAN sich befindet, weiter. Zusätzlich leitet das MTEP die ARP Anfrage an die Mulicast Adresse der Gruppe weiter. Der Switch des SubnetB übermittelt das ARP Paket an weitere Teilnehmer. Hier ist das der ESXi4 mit der VM4. [44, S.40-41]

NSX Firewallvarianten

Ein weiteres Argument zum Einsatz eines SDN ist die granulare Reglementierung des Datenverkehrs. Zur Regulierung stehen dem Administrator bei NSX, zwei zentrale Instrumente zur Verfügung. Zum einen gibt es in den Edge Services und DLRs mit einer integrierten Firewall zur Absicherung der Perimeter Grenze. Die virtuellen Instanzen werden von der Distributed Firewall (DFW) geschützt. Bei dem Einsatz dieser beiden Optionen wird im Normalfall keine „Entweder-Oder-Strategie“ gefahren, sondern parallel eingesetzt. Hierbei bildet die EdgeService Firewall die Perimeter Grenze zur physikalischen Welt. Sie wird also genutzt um den „North-South-Traffic“ zu überwachen. Die DFW dagegen wird pro virtuellen Adapter einer virtuellen Maschine instanziiert. Dies bedeutet, dass jedes empfangene oder gesendete Datenpaket einer VM die Firewall durchläuft, inspiziert und nach dem aufgestellten Regelwerk beurteilt wird. Bei der DFW kommen dabei zwei Tabellen zu tragen. Die erste Tabelle ist die „Connection Tracker Table“ [44, S.30], hierin wird jeder schon bekannte Datenverkehrsfluss protokolliert und dokumentiert. Der Vorteil der hieraus entsteht, ist:
ein Kommunikationsfluss bekannt und erwünscht, muss dieser nicht bei jeder erneuten Sendung das Firewallregelwerk durchlaufen. Ist ein Kommunikationsfluss noch nicht bekannt, wird die Regeltabelle der Firewall durchlaufen. Stellt sich dabei heraus, dass es keine verwerfende oder ablehnende Richtlinie gibt, wird diese Kommunikation in die „Connection Tracker Table“ übernommen und der Datenverkehr erlaubt. Bei einer erneuten Sendung muss nicht nochmal erneut das Regelwerk durchlaufen werden. Beim Blockieren des Datenflusses wird kein Eintrag erstellt. Bei einem erneuten Sende-

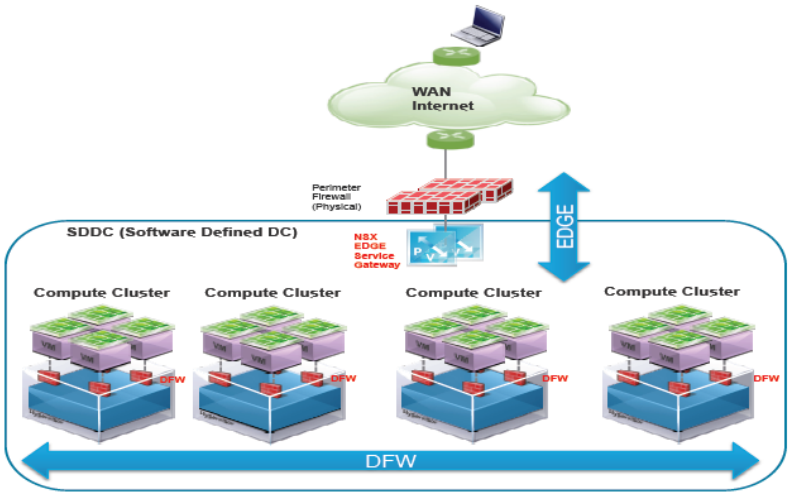

Abbildung 1.7: NSX Firewall Architektur [44, S.26]

/Empfangsvorgang muss also erneut das Regelwerk der Firewall abgearbeitet werden. Die DFW wird zur Absicherung des „East-West-Traffic“ verwendet, siehe hierzu Kapitel 1.4. Bei der Erstellung neuer Sicherheitsrichtlinien können VMware Objekte, wie logische Switche, das VM-Objekt oder klassische Objekte wie IP-Adressen verwendet werden. Mit der DFW ist es möglich in Layer2-4 Traffic einzusehen und zu kontrollieren. Werden z.B. VMware Objekt wie die virtuelle Maschine verwendet oder logische Switche ist es möglich Datenverkehr innerhalb eines Netzwerksegmentes zu beeinflussen. Dies wird auch daraus ersichtlich, dass die DFW auch ein „redirecting“, also die Umleitung eines Datenstroms veranlassen. Ein „redirecting“ ermöglicht die gezielte Umleitung eines Datenstroms zu einer weiteren Drittherstellerlösung, welcher diesen überprüfen und beeinflussen kann. Der Einsatz von Dritthersteller Software hat das Ziel erweiterte Schutzfunktionen zu implementieren. Bei VMware werden diese Dienste „advanced network security services“ [44, S.77] genannt. Die Abbildung 6 stellt die Firewallstruktur beider Komponenten dar. [44, S.25-32, 75-78]

Der nutzbare Funktionsumfang von VMware NSX ist abhängig von der verwendeten Lizenz. Aktuell gibt es vier Lizenzstufen: Standard, Advanced, Enterprise und Robo. Auf eine genaue Gegenüberstellung und Einsatzzwecke wird an dieser Stelle verzichtet. Zum Betreiben einer Mikrosegmentierung können die Lizenzen Advanced, Enterprise und ROBO verwendet werden. Die Funktion des L2VPN ist nur in der Enterprise und ROBO Lizenz erhalten. [19]

1.3 Das Zero Trust Model

Das Zero Trust Model wurde im Jahre 2009 wurde von John Kindervag und seinen Mitarbeiter am Forrester Research Inc. entworfen [6]. Dieses Model ist ein Leitfaden zum Umgang mit Daten und deren Absicherung in der Informationstechnologie, sowie

deren Systemen auf welchen diese Daten liegen. Die Darstellung dieses Modells soll auf zwei Ebenen erfolgen. Zum einen welche die grundlegenden Ansätze des Zero Trusts Modells sind. Im zweiten Teil werden diese Grundsätze zur Gestaltung eines „Zero Trusted Networks Architecture“ (ZTNA) verwendet. Das Zero Trust Modell kann auf geschäftliche Prozesse für den Datenschutz und die -sicherheit angewendet werden [35, S.8-9]. Diese sollen an dieser Stelle jedoch nicht berücksichtigt werden.

1.3.1 Grundlagen

Grundsätzlich bedeutet Zero Trust nur eines – „In Zero Trust, all network traffic ist untrusted“ [34, S.2] – diese bedeutet innerhalb eines Netzwerkes gibt es keinen vertrauenswürdigen Datenverkehr. Dies ist im Vergleich zu bestehenden Konzepten wie dem „Trust, but verify“ [35, S.4] Modells ein gegengesetzter Ansatz. Ziel und Quelle spielen dabei prinzipiell keine Rolle. Das Grundkonzept des Zero Trust Models besteht aus drei Merkmalen:

- Sicherstellung eines gesicherten Zugriffes auf Ressourcen
  Jeglichen Zugriff auf Ressourcen unterbinden, welche nicht von der kontrollierenden Instanz des Unternehmens zugelassen wurden. Diese kann durch eine Dateiverschlüsselung und verschlüsselte Tunnel für den Dateizugriff gewährleistet werden. [35, S.5]
- strengste Dateizugriffskontrollen mit minimalen Zugriffsberechtigungen
  Anwender haben nur Zugriff auf notwendige Ressourcen. Um diese zu gewähren kann z.B. ein rollenbasiertes Zugriffsverfahren verwendet werden. [35, S.5]
- Protokollierung und Auswertung
  Wichtig ist die Protokollierung und Auswertung des Netzwerkverkehres. Daten müssen gesammelt und inspiziert werden, sodass auffälliges Verhalten gleich erkannt wird und Gegenmaßnahmen getroffen werden können. [35, S.5]

1.3.2 Zero Trust Netwerkarchitektur

Eine ZTNA beansprucht für sich eine völlig neue Herangehensweise des Aufbaus eines Netzwerkes zu sein [35, S.5]. Wichtige Elemente einer ZTNA sind Segmentierung, zentrale Verwaltung, Parallelisierung Protokollierung und Analyse des Datenverkehrs. Häufig wird dabei nur das Augenmerk auf die Perimeter Grenze gelegt. Hiervon ausgehend werden die groben Segmente wie Wide Area Network (WAN), Demilitarisierende Zone (DMZ) und interne Netze entworfen und sicherheitstechnisch vorbereitet. Die Planung beginnt meistens an dieser Grenze. Die Folge ist, dass das Sicherheitskonzept hierunter leidet. An dieser Stelle werden viele mit Sicherheitsfunktionen installiert, welche einen hohen Kostenaufwand nach sich zieht. Eine solche Netzwerkstruktur wird auch „hierarchisch“ [34, S.3] bezeichnet. Gelingt es Angreifern durch dieses Konstrukt durchzubre-

chen sind häufig nur noch geringe Hürden zu überwinden. [34, S.2-5] Das hierarchische Modell besteht aus drei bzw. vier Elementen, der Kante (Perimeter Grenze), dem Kern oder Rückgrat, optional aus einer Verteilungsebene und den Zugriffspunkten.

- Perimeter Grenze/Kante - Edge
  Ausbruchsstelle für interne zu externen Netzwerke. Kontrollierende Instanz für eingehende und ausgehende Datenpakete zwischen diesen beiden Segmenten. [34, S.3]
- Kern/Rückgrat – Core/Backbone
  Besteht aus einer Komponente, welche die zentrale Weiterleitungseinheit für Datenpakete innerhalb einer Organisation darstellt. Diese Einheit ist mit dem Internet verbunden. Elementare Sicherheitsfunktionen werden in dieser Ebene implementiert. [34, S.3]
- Verteilungsebene - Distribution
  Distribution Komponenten stellen eine Verbindung zwischen den Core Element und den Zugriffspunkten her. Diese Komponenten waren häufig leistungsfähige Switche, welche z.B. einzelne Zugriffspunkte in logische Segmente einteilten und diese dann mit dem Core Switch verbunden hatten. Heutzutage gibt es aufgrund der leistungsstarken Core Switche oder der Unternehmensgröße Implementation bei welchen auf Distributions Komponenten verzichtet wird. [34, S.4]
- Zugriffspunkten – Access
  Die Access Komponenten bilden die Schnittstelle für Endgeräte sich an dem Unternehmensnetzwerk anzubinden. Implementierte Sicherheitsfunktionen an diesem Zugang sind den meist Network Access Protection (NAP) oder Firewalls (FW). [34, S.4]

Bei dem Ansatz der ZTNA wird die Sicherheit des Netzwerkes schon bei der Planung berücksichtigt und erhöht. Dabei gilt es zu beachten, dass das ZTNA eine „theoretische Adaption des Zero Trust Models für Informationssicherheit“ [34, S.7] ist. Daher bedient sich das Modell an Elementen, welche unter den genannten Produktbezeichnungen eventuell so nicht im Handel erhältlich sind. Nach dem ZTNA wird empfohlen erst die Endpunkte (Server, Speicher, Computer, etc.) zu planen und danach die einzelnen Anbindungen zu entwerfen. Somit wird zuerst versucht die Daten oder Informationen logisch in ein Segment einzuordnen und danach die einzelne Vernetzung und Sicherheitsrichtlinien anhand der zu verbindenden Segmente zu entwerfen. Der Entwurf sieht dabei vor, dass durch die neuartige Planung anstatt einem sehr leistungsstarken Coreswitch mehrere kleinere Switche verwendet werden. Durch die Verwendung mehrerer Switche können auch Optimierungen am Datenverkehr vorgenommen werden wie der Einsatz von multiplen Routen zu einer Destination. Die Auswahl der zu verwendenden Route kann dabei abhängig von der Auslastung oder Effektivität sein. Wird diese Strategie konsequent angewendet, wächst ein Netzwerk von innen nach außen, an welchem als letzte Anbindung der Ausbruch ins Internet umgesetzt wird, die Perimeter Grenze. [34, S. 2-5]

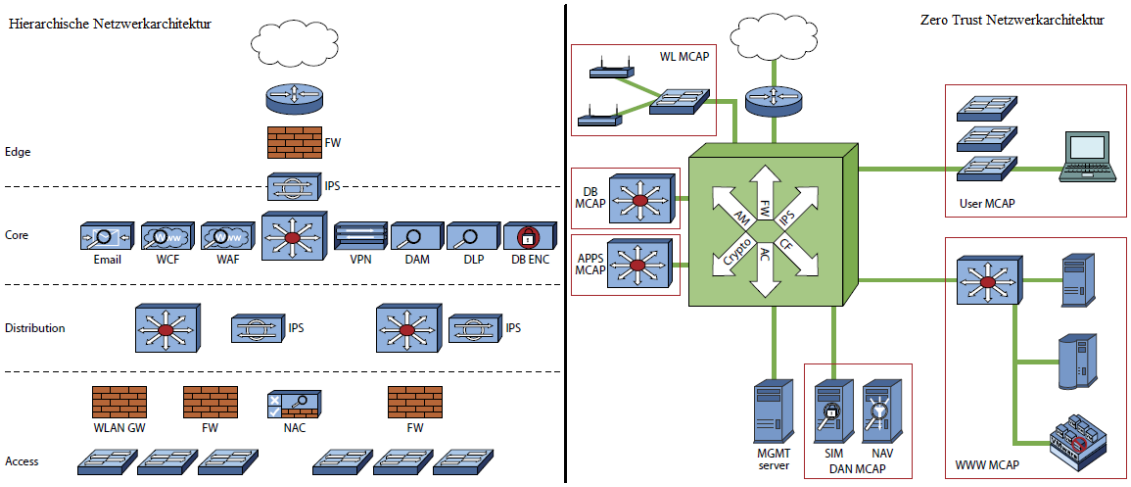

Abbildung 1.8: Gegenüberstellung hierarchisches Modell und ZTNA basierend auf [34, S.26]

Für die Umsetzung eines ZTNA wird ein zentrales Element in einem Netzwerk installiert, in welchem alle Sicherheitskomponenten implementiert sind. Dieses Element wird nach Kindervag „segmentation gateway“ (SG) [34, S.7] genannt. Durch die zentrale Positionierung einer solche Komponente soll sichergestellt sein, dass jeder segmentübergreifende Datenverkehr durch entsprechende Sicherheitskomponenten kontrolliert und überwacht werden kann. Für die Umsetzung des zweiten Merkmals eines ZTNA, der Segmentierung, steht eine sogenannte „microcore and perimeter“ (MCAP) [34, S.8] zur Verfügung. Eine MCAP reguliert den ein- und ausgehenden Datenverkehr eines Segmentes und ist mit einer SG verbunden. Sie erhält von der SG globale Sicherheitsrichtlinien zum Schutz des Segmentes. Aufgrund der logischen Zuordnung von Objekten, basierend auf deren Funktionalität, können die globalen Richtlinien für diese Objekte des jeweiligen MCAP übernommen werden. Somit bildet jedes Segment eine isolierte Umgebung, welche nur über ein SG angesprochen werden kann und in welchem für die interne Sicherheit Richtlinien bestehen.
Die Nutzung eines zentralen Verwaltungssystems für die Umgebung ist das dritte Merkmal einer ZTNA. Für die Administration der Komponenten gibt es eine Oberfläche, welche sich von dem veralteten Standard des Command Line Interface (CLI) verabschiedet und eine graphische Oberfläche dem Administrator anbietet bzw. eine API für die automatisierte Administration bereitstellt. Als ein weiteres essentielles Merkmal einer ZTNA wird das Protokollieren und Analysieren von Datenverkehr angesehen. Das Ziel ist jeden Datenverkehr an jedem einzelnen MCAP einzufangen und zu untersuchen. Dies kann und wird nicht von einem menschlichen Mitarbeiter durchgeführt, sondern geschieht automatisch. [34, S.9]
Hierfür steht dem Administrator folgende Komponenten zur Verfügung, eine sogenanntes „security information management“ (SIM) [34, S.9] und eine „network analysis and visibility “ (NAV) [34, S.9] Anwendungen zur Verfügung. „Ein SIM-System sammelt Daten an einer zentralen Stelle zur Analyse und bietet die automatisierte Erstellung von Berichten, . . . , sowie ein zentralisiertes Berichtswesen.“ [11]. NAV Anwendungen visualisieren Netzwerkverkehr um z.B.: Engpässe zu analysieren oder anhand von ana-

lysierten Paketen Schadcode zu erkennen [30, S.2]. Für die Protokollierung und die Analyse dieser Informationen sieht eine ZTNA ein separates Netzwerk vor. Dieses wird als „Data Acquisition Network“ (DAN) [34, S.8] genannt. Innerhalb dieses Netzwerkes würden dann alle Protokolle zur Überwachung und Analyse wie Syslog oder Simple Network Management Protocol (SNMP) übertragen werden. [34, S.8]

Aufgrund dieser Merkmale ist eine ZTNA erweiterbar, skalierbar, mandantenfähig und lässt sich in bestehende Architekturen integrieren, sodass bei einer geplanten Umsetzung diese schrittweise durchgeführt werden kann. Eine Gegenüberstellung eines ZTNA und einem hierarchischen Modell ist in der Abbildung 1.8 aufgezeigt. [34, S. 12-14]

1.4 Definition einer kritischen Infrastruktur

Die Titulierung dieser Arbeit enthält den Ausdruck „kritische Infrastruktur“, welcher bei objektiver Betrachtung eventuell eine falsche Zielgruppe vermittelt. Der Begriff einer kritischen Infrastruktur wird innerhalb des Bundes wie folgt definiert:
„Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“ [25, S.3]

In einem privatwirtschaftlichen Kontext wird der Terminus einer „kritischen Infrastruktur“ für Bereiche angewendet die meistens unternehmenskritisch sind. Ausfälle oder Kompromittierung von Daten in diesem Bereich können bei einem Unternehmen zu irreparablen und existenzgefährdenden Schäden führen. Häufig ist es auch schon ausreichend wenn ein Angreifer Zugriff auf diesen Bereich hat und die Kommunikation innerhalb dieser Zone mitlesen und aufzeichnen kann. In dieser Arbeit bezieht sich der Begriff einer „kritischen Infrastruktur“ hauptsächlich auf das privatwirtschaftliche Umfeld.

1.5 Mikrosegmentierung

Der Begriff der Mikrosegmentierung ist relativ neu eingeführt worden. Die Idee dahinter bezieht sich auf das zuvor beschriebene Zero Trust Model [36, S.19]. Die Mikrosegmentierung verfolgt das Ziel Datenverkehr sehr granular zu reglementieren. Der Wunsch danach war schon davor gegeben, jedoch technisch oder aufwandsmäßig nicht immer realisierbar. [36, S.27] Heutige Netzwerkentwürfe haben häufig Ihren Sicherheitsschwerpunkt auf die Absicherung der Perimeter Grenze. Als Perimeter Grenze wird der Übergang zwischen internem Netzwerk in das externe Netzwerk bezeichnet. Sie ist damit die Grenze zwischen dem zu verwaltenden/e Netzwerk/e in Netze, in welchen keine Einflussmöglichkeiten bestehen. Ist diese Grenze jedoch einmal durchbrochen worden, greifen häufig nur noch wenige Sicherheitsmechanismen auf der Netzwerkebene. [36,

S.6] Die Endsysteme sind an dieser Stelle dann häufig „auf sich alleine gestellt“. Der Aufbau und das Nutzen einer SDN Umgebung zur Realisierung einer Mikrosegmentierung sollen nachfolgend erörtert werden.

1.5.1 Segmentierung von Netzwerkdatenverkehr

Die Segmentierung von Netzwerkdatenverkehr ist die Unterteilung von Systemen in verschiedene isolierte Kommunikationsbereiche. Diese Einteilung kann auf verschiedene Kriterien beruhen und ist keine neue Herangehensweise. Standardmäßig werden Systeme aufgrund Ihres Anwendungszweckes eingeteilt. Segmente, welche für Geschäftsprozesse miteinander kommunizieren müssen werden durch Komponenten wie Routern verbunden. Um eine Überprüfung des Datenverkehrs nun zu bewerkstelligen besitzen diese Komponenten Mechanismen wie Firewalls oder Router mit Access Control Lists (ACL). In einem klassischen TCP/IP Netzwerk gelangt der Datenverkehr nur an diese Prüfpunkte, wenn das Netzwerksegment gewechselt wird. Die Regulierung des Netzwerkverkehrs innerhalb eines Segmentes ist auf Netzwerkebene nicht möglich. Hierzu müsste am Client separate Schutzvorkehrungen, z.B. in Form einer Desktop-Firewall, getroffen werden. Das Problem heutiger Segmentierungen ist, dass Segmente häufig sehr groß dimensioniert werden. Eine effektivere und sichere Variante der Segmentierung wäre die der Einteilung nach Arbeitsprozessen. Leider kommen genau hier die zuvor angesprochenen Schwierigkeiten zum Tragen. In großen Umgebungen sind häufig viele kleine Segmente nicht realisierbar, da nicht genügende Adressräume für die logische Unterteilung zur Verfügung stehen. Ein weiteres technisches Hindernis ist der Datenverkehrsfluss. Es müsste in eine große Anzahl an Sicherheitskomponenten, wie Routern oder Firewalls, investiert werden um den Datenverkehr granular zu regeln bzw. die Durchsatzraten und Latenzzeiten zu gewähren. Bei einer großen Anzahl an Sicherheitssystemen, egal ob es sich dabei um Desktop- oder dedizierte Netzwerk-Firewalls handelt, ist der administrative Aufwand sehr hoch um Datenverkehr gezielt zu filtern. Die grundlegende Problematik des Überprüfens von internen segmentären Datenverkehrs bleibt jedoch weiterhin bestehen. Durch die Bildung von vielen kleinen Segmenten wurde zwar die Broadcastgröße verkleinert und der übergreifende Segmentverkehr erhöht. Hierdurch kann Datenverkehr eines Geschäftsprozesses in unterschiedliche Segmente umgeleitet werden und wird dadurch überprüfbar. Erfüllt aber trotzdem noch nicht die Ansprüche einer Mikrosegmentierung. [36, S.10-11] Damit eine Umgebung als Mikrosegmentiert gilt sollten folgende Anforderungen erfüllt sein:

- Isolation und Segmentierung
  Eine Bildung von mehreren kleinen Netzwerksegmenten, welche autark und isoliert voneinander betrieben werden können. Die Segmente sind dabei erweiterbar, aber Restrektionen bleiben beständig. [36, S.53]
- Öffnung nur notwendiger Kommunikationswege und Kontrolle
  Basierend auf den Zero Trust Anforderungen wird die Kommunikation so stark re-

guliert, dass nur notwendige Dienste und Endgeräte miteinander kommunizieren können. Dies gilt auch für Objekte innerhalb eines Segmentes. [36, S.53]

- Allgegenwärtig und zentrale Administration
  Die Administration der Umgebung erfolgt von einem zentralen Ort. Sicherheitseinstellung sind allgegenwärtig an ein Objekt gebunden. Die Automation von Netzwerkanlage und Kategorisierung von Objekten, sowie deren Zuordnung von Sicherheitsrichtlinien, ermöglichen einen ständigen Schutz von der Erstellung bis zum Entfernen eines Objektes. [36, S.53]

1.5.2 Komplexität durch 'North-South' und 'East-West' Traffic

Die Begrifflichkeiten des „North-South“ und „East-West“ Traffic sollen die bildliche Vorstellung von dem Fluss der Datenpakete geben. Der „North-South“ Traffic wird als Datenverkehr bezeichnet, welcher zwischen der physikalischen und der virtuellen Welt aufkommt bzw. auch Datenverkehr zwischen externen und internen Netzen. „East-West“ bezeichnet den Datenverkehr zwischen und innerhalb der logischen Netzwerke, sowie internen Datenverkehr, wie zwischen zwei Servern. [36, S.17]

Angesichts der Anforderungen und Kernelemente einer Mikrosegmentierung sollten beide Kommunikationswege bestmöglich reguliert sein. Konflikte und Überschneidung des Regelwerks können hierdurch auftreten und eine Fehlersuche erschweren.
In diese Komplexität reihen sich ebenfalls die „advanced security services“ [44, S.78] ein. Die advanced security services bieten die Möglichkeit Drittherstellern von erweiterten Sicherheitslösungen zusätzlichen Schutz des Datenverkehrs einer VM zu gewähren. Solche Lösungen werden eingesetzt um einen AntiMalware Schutz auf den VMs zu gewährleisten oder zur Überprüfung des Netzwerkverkehrs um Datenpakete auch in oberen Ebenen des OSI Schichtenmodells zu überprüfen. Infolge eines Einsatzes dieser Dienste, ergibt sich eine weitere Schnittstelle mit welcher die Komplexität einer Mikrosegmentierung erhöht. [44, S.77-79]

1.5.3 Herausforderungen bei der Implementierung

Bei der Implementierung einer Mikrosegmentierung sind mehrere Aspekte zu beachten. Wie aus den vorigen Kapiteln hervorgegangen ist, bedeutet eine granulare Regulierung sehr viel Aufwand. Datenflüsse müssen beachtet werden und anhand seiner Anwendungsinhalte reglementiert werden. Dies ist eine große Schwierigkeit in heutigen Netzen. Es existieren viele Anwendungen, die auf unterschiedliche Ressourcen in internen oder externen Netzwerken zugreifen. Um diese zu erkennen und herauszufiltern welches eine erwünschte Kommunikation ist, ist es wichtig seinen Netzwerkverkehr vor der Implementierung genau zu untersuchen. Grundlegend sollten folgende Punkte dabei beachtet werden:

- Datenfluss verstehen
  Beim Planen einer SDN Umgebung, wird empfohlen eine Übersicht über die aktuelle Vernetzung zu haben. Es sollten Nadelöhre erkannt werden und durch Equal-Cost-Multi-Path (ECMP) routing, Multicasting, dynamisches Routing und etc. optimiert werden. [36, S.55]
- Netzbeziehungen kennen
  Aktuelle Netzwerkbeziehungen sollten betrachtet werden, ob eine Verkleinerung der Segmente möglich ist. Der Einteilung der Segmente kann nach Aufgaben der Server, Anwendungsprozessen, Mandanten oder weiteren Klassifikationen erfolgen. [36, S.56]
- kritische Infrastrukturen erkennen und restriktive Abschottung
  stark gefährdete Bereiche wie Virtual Desktop Infrastructures (VDI) erkennen und eventuell erweiterte Schutzmaßnahmen mit advanced security services umsetzen. [36, S.58]
- Erstellen eines Sicherheitsrichtlinienmodells
  Auf Basis der erlangten Erkenntnisse des Datenflusses und Netzbeziehungen kann ein Sicherheitsrichtlinienmodell erarbeitet werden. Sicherheitsrichtlinien sind die Regeln, an den einzelnen Komponenten wie Edge Services, DFW und Advanced Security Services implementieren. Eine Mikrosegmentierung versucht immer eine nahe Umsetzung des Zero Trust Models, was bedeutet das in dieser Umgebung eine Deny-All Strategie gefahren werden sollte. Deny-All - grundsätzlich wird jeder Datenverkehr verhindert. Er muss explizit über das Regelwerk freigegeben werden. [36, S.55]

2 Methodenteil

Innerhalb der folgenden Kapitel werden die vorgenommen Einstellungen zum Erreichen einer Mikrosegmentierung innerhalb eines SDN auf Basis von VMware und VXLAN beschrieben. Als Orientierung diente folgende Anleitungen von VMware: VMware Validated Reference Architecture Guide 2.0, VMware Network Virtualization Design Guide, Microsegmentation Using NSX Distributed Firewall

2.1 Aufbau der Server- und Netzwerkinfrastruktur

Die physische Infrastruktur umfasst die Beschreibung der Netzwerkkomponenten und der physischen Serverkonfiguration der NSX Projektkomponenten. Da diese Umgebung auch als Demonstrationsumgebung für Kunden dient, wurden die Komponenten in einer redundanten Form, eines Clusters, ausgelegt. Hierbei wurden die vorhanden physischen Server auf drei Cluster mit jeweils zwei Knoten aufgeteilt. Das Clusterdesign entspricht dabei den Empfehlungen von VMware [42, S.108-110]. Ausnahme hierbei bildet das Managementnetz, welches nicht in einer virtuellen Umgebung abgebildet worden ist, sondern als physisches Netzwerk entworfen wurde. Dies lag an der Gestaltung eines eigenständigen Managementnetzes, in welchem weitere externe Komponenten und zusätzliche Server, wie der Management Server, eingebunden werden sollten. Der Management Server wird für administrative Tätigkeiten genutzt. Die aus den vorhanden Ressourcen entstandene Verteilung an Hardware und der Knoteneinteilung je Cluster, kann der Abbildung 9 entnommen werden. Bei der Zuweisung von Hardwareressourcen wurden jedem einzelnen Knoten eines Clusters, jeweils die gleiche Anzahl und Art der Komponenten zugewiesen. Das EdgeRoute-Cluster dient als Ausbruchsstelle aus der virtuellen in die physikalische Netzwerkumgebung. Ein solches Ausbruchsszenario kann auch anderweitig, wie mit externer Hardware, realisiert werden. Dies ist aber nicht Bestandteil dieser Arbeit. Alle verwaltenden Instanzen wie vCenter Server, NSX Manager, etc. werden in dem ManagementCluster zur Verfügung gestellt. Die einzelnen fiktiven Mandantenumgebungen werden in dem ComputeCluster installiert und ausgeführt. Zu guter Letzt dient der Managementserver als zentraler Anlaufpunkt für die Administration. Für die Festplattensysteme wurden unterschiedliche Herangehensweise zur ausfallsicheren Betreibung gewählt. Für das ComputeCluster wurden die externen Storages mit Hilfe von Fibre Channel gekreuzt an die einzelnen Knoten angeschlossen. Mit gekreuzt ist gemeint, dass in jeder Storage und in jedem Server des Clusters jeweils zwei Fibre Channel Karten eingebaut sind. Eine Schnittstelle der Storage ist mit dem ESX Server 05 und die andere Schnittstelle ist mit dem ESX Server 06 verbunden. Dies gilt auch für die zweite Storage. So steht die Storage beiden Servern zur Verfügung und im Falle einer Verlagerung aus Leistungs- oder Ausfallsgründen bleibt die Ressource des Festplattenspeichers weiterhin der virtuellen Instanz nutzbar. Für das EdgeRoute-

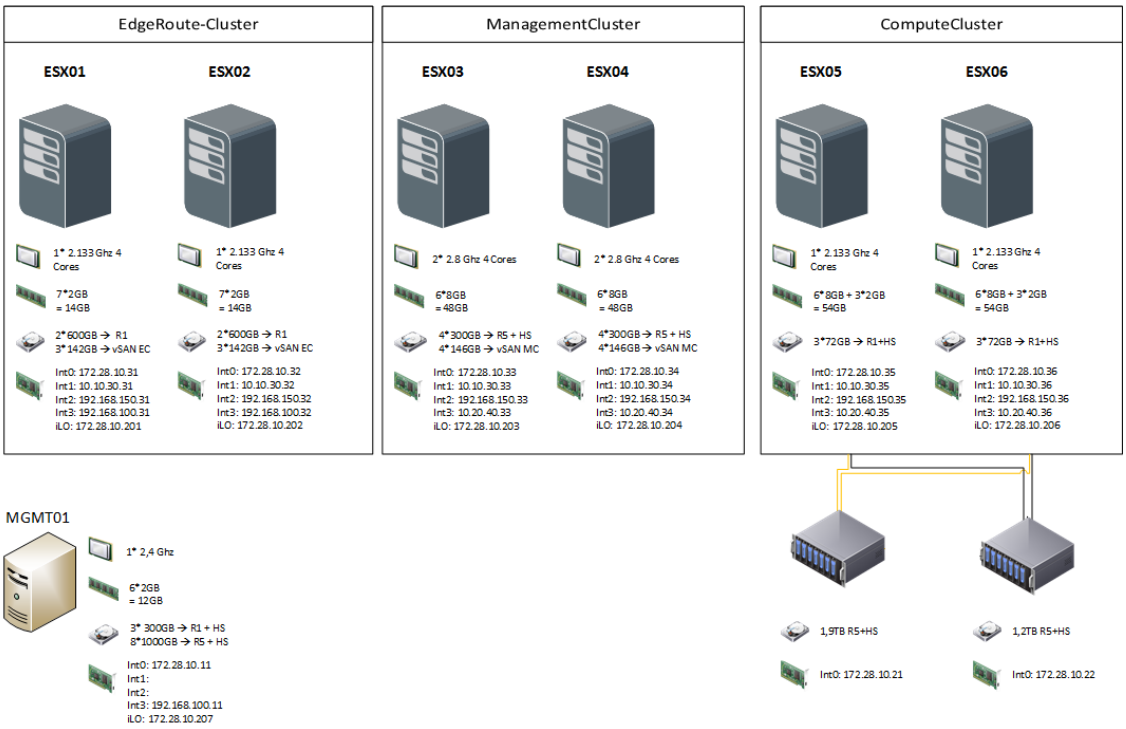

Abbildung 2.1: Hardwareressourcen Verteilung Laborumgebung, Eigenerstellung]

Cluster und dem Management-Cluster wurde die Redundanz durch die Bereitstellung einzelner Festplatten in den Servern und einer Bildung eines Festplattenclusters auf Basis von VMware vSAN realisiert. Hierauf wird im nachfolgenden Kapitel näher eingegangen. Für die Vernetzung der Serversysteme wurden dabei zwei Cisco Catalyst Switche im Cluster und ein FortiGate Cluster als Router verwendet. Das FortiGate Cluster stellt dabei einen zentralen Ausbruchspunkt ins Internet dar. Für das Transportnetz wurde ein zusätzlicher HP ProCurve Switch installiert. Dies ist nötig geworden da eine Größenzuweisung der MTU je VLAN auf den vorhandenen Cisco Switche technisch nicht realisierbar ist. Die Erhöhung der MTU (Maximum Transmission Unit) ist für den Betrieb eines Transportnetzes, basierend auf VXLAN, jedoch unerlässlich. Nachfolgend einen kurzen Überblick über die physischen Netze der NSX Umgebung, sowie deren Verwendungszweck:

- vMotion-Netz (10.10.30.0/24) – VLAN ID 991
  vMotion nennt sich die Technik welche die Verschiebung virtueller Instanzen auf verschiedene ESXi Hosts verwaltet und durchführt. Um den Netzwerkverkehr zu verringern wird empfohlen ein eigenes Netz für dieses System bereitzustellen.
- vSAN-Netz (10.20.40.0/24) – VLAN ID 992
  vSAN wird das Produkt von VMware genannt, welches für die Virtualisierung von Festplattenspeicher über mehrere ESXi Hosts dient.
- Transportnetz (192.168.150.0/24) – VLAN ID 993
  Wie beschrieben ist VXLAN eine Overlaytechnologie. Dies bedeutet es wird ein grundlegendes IP Netzwerk benötigt auf welchem die Daten physisch transpor-

tiert werden können.

- Breakout/Uplink (192.168.100.0/24) – VLAN ID 996
  Mit Breakout und Uplink wird der Ausbruch aus der virtuellen in die physische Netzwerkumgebung verstanden. Dabei dient das EdgeRoute Cluster als „Ausbruchsort“ und ist über das 192.168.100.0/24 mit der FortiGate für z.B. die Internetkonnektivität verbunden.
- Managementnetz (172.28.10.0/24) – VLAN ID 999
  Dient zur Verwaltung der einzelnen Komponenten des Netzwerkes. Aus diesem Netz werden administrative Tätigkeiten durchgeführt.

Die virtuelle Netzwerkumgebung wird im Kapitel 2.1.3 fiktive Kundenumgebung genauer beschrieben.

2.1.1 Konfiguration der VMware Komponenten

Im Folgenden wird näher beschrieben, wie sich der grundlegende VMware Aufbau in dieser Testumgebung zusammensetzt.

vSphere-Cluster
Die vSphere Server wurden in ein Cluster mit jeweils zwei Knoten eingeteilt. Bei der Aktivierung der Dienste wurde das automatische DRS (Distributed Ressource Scheduler) aktiviert. Durch die Aktivierung dieser Funktion werden Verschiebungen von virtuellen Instanzen aufgrund von Lastenverteilung automatisch vorgenommen. Hierdurch werden z.B. nach der Erstellung einer neuen VM, die VMs lastengerecht auf die Hosts des Clusters verteilt. Als letzte Option ist für jedes Cluster der Funktion der High Availability konfiguriert. Hierdurch werden bei einem Ausfall automatisch die virtuellen Instanzen auf den anderen Knoten verschoben. [17, S.18]

vSAN-Cluster
Innerhalb des vSAN werden einzelne Festplatten eines Knoten markiert und mit den anderen Festplatten anderer Knoten eines Clusters in eine virtuelle Festplatte zusammengefasst. Die Anbindung der Server sollte daher auch dementsprechend ausgelegt sein. Es werden 1 GBit Anbindungen unterstützt [27, S.20] waren aber in der Laborumgebung teils schon nicht mehr ausreichend um VMs auf dieser Basis zu betreiben. Da es sich um ein zwei Knoten Cluster handelt ist für die Vermeidung eines „Split-Brain Szenarios“ [17, S.30] die Einrichtung eines Zeugenhosts (witness host) je vSAN Cluster nötig. Als Zeugenhost wurden in dieser Umgebung nested ESXi-Server für die beiden Cluster verwendet. Hierzu bietet VMware vorgefertigte und lizenzierte Appliances. Bei der Nutzung von vSAN kam es im Testbetrieb des Management-Clusters zu Leistungsengpässen bei der Datenübertragung der VMs, weshalb hier für die kritischen VMs auf die lokalen Storages ausgelagert wurden. Die Ausfallsicherheit wird dann durch die Verlagerung der VMs auf die lokalen RAID Systeme sichergestellt und im Falle eines Ausfalls

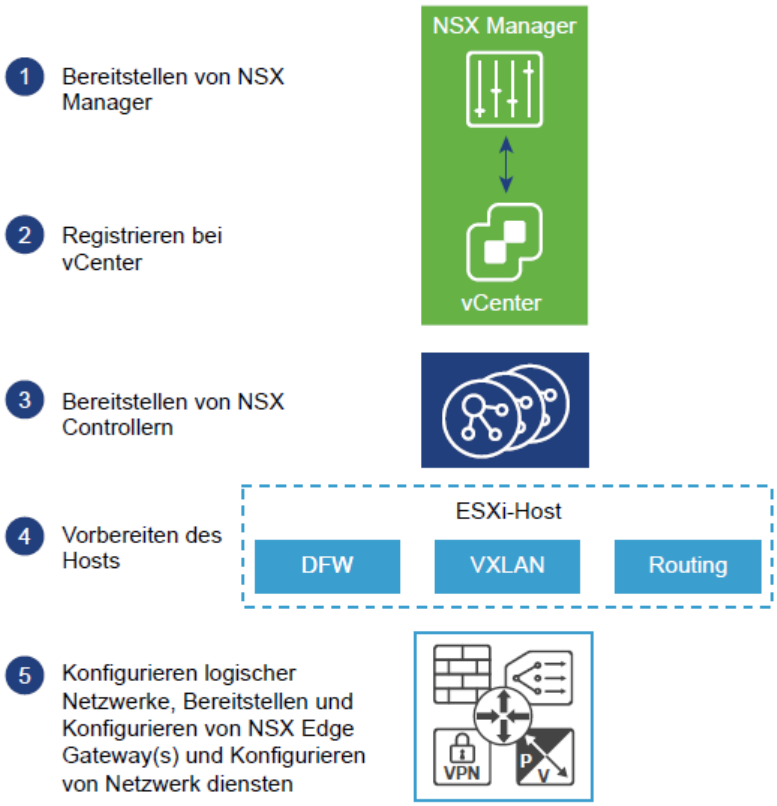

Abbildung 2.2: VMware NSX Workflow Implemtierung, [46, S.29]

der physischen Maschine durch ein Backup. Gelegentlich ist es bei manchen kritischen VM Systemen sinnvoll, diese mehrmalig auszurollen und als virtuelles Cluster zu betreiben. Hierdurch wird nochmals eine Ausfallsicherheit einer einzelnen VM sichergestellt. Die einzelnen virtuellen Knoten sind dabei auch auf unterschiedlichen physischen ESX Servern verteilt.

2.1.2 Implementierung einer SDN Umgebung mit NSX

Für die Bereitstellung einer NSX Umgebung sind einige Vorarbeiten notwendig. Zum einen muss eine physische und logische VMware Umgebung eingerichtet sein, was in den vorangegangenen Kapiteln beschrieben wurde und zum anderen müssen an teilnehmenden Netzwerkkomponenten Einstellungen angepasst werden. VMware hat eine „Workflow-Grafik “ zur Implementierung von NSX, welche in der Abbildung 2.2 dargestellt ist. In diesem Projekt wurden diese Schritte mit Hilfe des Installationshandbuches durchgeführt. Die Installation der NSX Komponenten geschieht dabei ausschließlich über das vCenter. Im ersten Schritt wurde die virtuelle Appliance des NSX Managers importiert und konfiguriert. Nach dem erfolgreichen Import werden die Grundeinstellung via Weboberfläche auf dem NSX Manager konfiguriert. Innerhalb dieser Oberfläche wird auch die Verbindung zum vCenter Server hergestellt. Sobald diese Verbindung erfolgreich steht, erscheint am vCenter Server ein neuer Funktionsreiter „Networking &

Security “, in welcher die weiteren Einstellungen vorgenommen werden. Im nächsten Schritt werden die NSX Controller installiert. Die VMs werden automatisch bei Auswahl des Installationsbuttons bereitgestellt. Es ist darauf zu achten, dass mindestens drei Instanzen installiert werden.
Die vorletzte Stufe bevor die Möglichkeit besteht virtuelle Netze in einer NSX Umgebung zu implementieren ist die sogenannte Hostvorbereitung. Es werden bei der Hostvorbereitung die an der virtuellen Netzwerkumgebung teilnehmenden ESXi Server mit den notwendigen Treibern für die VXLAN und Firewall Funktionalität ausgestattet. Diese Treiber werden VMware Installations Bundles (VIB) genannt. Für die aktuelle Umgebung wurde die Hostvorbereitung nur für die Knoten des EdgeRoute- und Compute-Clusters durchgeführt. Das Management-Cluster und damit auch das Managementnetz ist kein VXLAN unterstütztes Netzwerk.
Nachdem die ESXi Server nun in der Lage sind das VXLAN Protokoll zu verwenden, müssen noch die grundlegenden Konfigurationen zum Transport der Pakete konfiguriert werden. Hierfür wird die sogenannte Transportzone eingerichtet. Diese sagt aus, welche VXLAN fähige Geräte miteinander kommunizieren können. In dem Testszenario erstreckt sich die Transportzone über alle ESXi Server des EdgeRoute-Clusters und Compute-Clusters. Die Transportzone bildet die physische Grundlage zum Transport der VXLAN Pakete und nutzt das physikalische Netzwerk 192.168.150.0/24.
Somit sind das Edge-Cluster und Compute-Cluster die aktiven Teilnehmer der virtuellen Netzwerkumgebung. Das Management-Cluster stellt nur die Verwaltungsumgebung für das virtuelle Netzwerk zur Verfügung.
Mit der Bereitstellung der Transportzone ist die Grundinstallation abgeschlossen und es kann nun mit der Implementierung der virtuellen Netze begonnen werden. Es ist jedoch noch zu beachten, dass mit der Installation der Hostvorbereitung die DFW aktiviert wird. Standardmäßig ist sie jedoch nach der Installation in einem „alles Zulassen“ Modus vorkonfiguriert. Daher hat sie direkt nach der Installation keine Auswirkung auf die Kommunikation der virtuellen Maschinen, allerdings auch keine schützende Wirkung. Aus diesem Grund sollte sich im Vorfeld Gedanken zur Absicherung des Netzwerkverkehrs gemacht werden, der nach Zero Trust in einem SDDC differenziert angegangen werden kann, als vielleicht in klassischen Netzwerkarchitektur. Innerhalb dieser Testumgebung, ist eine gemischte Form der Herangehensweise gewählt worden, bzw. durch die Darstellung von Mandantenumgebungen besteht die Möglichkeit unterschiedliche Szenarien zu implementieren.

2.1.3 Einrichtung einer fiktiven Kundenumgebung

Nach der Bereitstellung der einzelnen NSX-Komponenten wurde eine fiktive Multimandantenumgebung erstellt. Die Kundenumgebungen wurden auf dem Compute-Cluster erstellt. Durch das Darstellen mehrerer Umgebungen sollen die Möglichkeiten einer SDN Umgebung und mögliche Ansätze aufgezeigt werden eine Mandantenfähigkeit abzubilden. In dieser Umgebung wurden alle Varianten VMwares, welche als „Best Practi-

ce[2] “ klassifizierten worden, umgesetzt.

1. Variante: Edge - Kundennetz
   Die einfachste Variante bietet sich für sehr kleine Mandanten oder für einen größeren Mandanten an. Hierbei steht eine Edge einem Kunden komplett zur Verfügung, da die Netzwerkstruktur oder die Anzahl der Dienste es verlangt. Alternativ werden an einer Edge an jeder Schnittstelle ein Netz unterschiedlicher Kunden konfiguriert. Da gilt es zu beachten, dass einer Edge nur maximal zehn Schnittstellen zur Verfügung stehen können.
2. Variante: Edge – Transfernetz – Kunden-DLR – Kundennetze
   Diese Variante ermöglicht an jeder Edge ein Transfernetz mit einer eigenständigen VNI zu erstellen und dieses mit einem DLR zu verbinden. Der DLR stellt die Schnittstelle zu den einzelnen Kundennetzen her. An einem DLR können bis zu 1000 interne und acht Uplink Schnittstellen konfiguriert werden. Daher muss in der Regel je Mandant ein DLR konfiguriert werden. An der Edge stehen weiterhin nur zehn Schnittstellen zur Verfügung, weshalb neun Schnittstellen als Transferschnittstellen für interne Mandanten genutzt werden können.
3. Variante: Edge – Transfernetz – Edges – Transfernetz – Kunden-DLR – Kundennetze
   Die letzte der drei Varianten ist die umfangreichste und bietet den Einsatz zusätzlicher Edges um deren Dienste gezielter oder differenzierter einzusetzen. Virtuelle Netzwerke mit einer solcher Umsetzung bieten nochmals den Grad einer höheren Abstrahierung von Mandantenlandschaften.

[44, S.69-72] Die Varianten sind in der Abbildung in der Anlage zu erkennen. Blau markierte Netzwerksegmente stellen dabei Transfernetze dar und grün hinterlegte Elemente sind kundenspezifische Netzwerke. Die CusB und BTH Umgebung stellen dabei die Variante 1 dar, Variante 2 wird durch die Kunden CusC, CusD und CusE dargestellt. Die letzte Variante wird durch die beiden zusätzlichen Edges Cus-edge02 & Cus-edge03 und den dahinter liegenden Mandanten cusy und cusz simuliert.

Als repräsentative Mittelstandskundenumgebung dient die BTH. In diesem Netzwerk existiert ein Verzeichnisdienst- (Active Directory), eMail- (Exchange), Datenbank- (Microsoft SQL) und Webserver (Microsoft Sharepoint) sowie drei Testclients und zwei Linux Server. Ebenso sind in dieser Umgebung mehrere virtuelle Netze eingebunden sowie dynamisches Routing aktiviert. Hierdurch soll ein realitätsnahes Szenario abgebildet werden. Diese vier virtuellen Netze haben folgende Aufgaben:

- Transfernetz (192.168.10.0/30)
  Stellt die Konnektivität zwischen Ausbruch (Edge Services) und internem Router dar.

[2] Best Practice bezeichnet im Allgemeinen, die empfohlene oder bewerte Herangehensweise an ein Thema

- Internes Servernetz (192.168.1.0/24)
  Server Netzwerk für sensible Serverdienste, welche vom Internet aus nicht erreichbar sein sollen, wie Active Directory oder Datenbank.
- Externes Servernetz (192.168.2.0/24)
  Netzwerk zur Bereitstellung von Server und Diensten, welche vom Internet aus erreichbar sein sollen.
- Client Netz (192.168.21.0/24)
  Netzwerk für Testclients.

Die dabei entworfene Struktur ist bewusst nicht auf einem „Zero Trust"- oder eines Mikrosegmentierungsansatzes basierend. Es wurde nur eine grobe Segmentierung der einzelnen Serversysteme vorgenommen. Dadurch ist es möglich eine Migration einer klassischen Umgebung in ein SDDC -Konzept zu simulieren. Eine 100% Simulation ist nicht möglich gewesen, hierzu wären einzelne physische Netzwerkkomponenten mit unterschiedlichen Sicherheitsfunktionen notwendig. Diese hätten im ersten Schritt analysiert und dann in ein Sicherheitsmodell auf eine SDDC Umgebung portiert werden müssen.

Bei den Mandantenumgebungen der Cus dienen die Mandanten CusB und CusC als einfache virtuelle Mandanten mit einem einfachen Netzwerk. Zur Darstellung der oben erwähnten 3. Variante wurden die CusY und CusZ gewählt. Hier aufgestellte Systeme sollen den Netzwerkverkehr einer solchen Mandantenumgebung transparent darstellen. Für die Demonstration einer Mikrosegmentierung wurden die Mandanten CusD und CusE gewählt. Dabei unterscheiden sich die Umgebungen im Folgenden. In der CusD Umgebung wurden drei Netzwerksegmente erstellt. Jedes Segment repräsentiert für seine enthaltenden Systeme eine Anwendungsgruppe. So existieren ein Datenbanksegment für Datenbankserver, ein Anwendungssegment für die Anwendungsserver und ein Websegment für die Webserver. In der CusE Umgebung existieren ebenfalls für eine Anwendungsgruppe jeweils ein Netzwerksegment. In diesem Fall ein Datenbank- und Webserversegment.
Die Unterschiede liegen bei der gewünschten Kommunikation einzelner Systeme inner- und außerhalb des Segmentes. Während in der CusD Umgebung jedes System in einem Segment mit anderen Systemen des Segmentes kommunizieren darf, ist in der CusE Umgebung die Kommunikation innerhalb eines Segmentes nur Systemen gestattet, welche einer Abteilung angehören. Aus diesem Grund existieren in den CusE Segmenten Server mit Kennzeichnung HR, für Human Ressources und FD, für Finance Department. Hierbei dürfen nur Abteilungsserver innerhalb und zwischen den Segmenten kommunizieren.
Die nachfolgende Tabelle gibt nochmals einen zusammenfassenden Überblick über die Ziele der einzelnen Landschaften in den Bereichen Netzwerkdesign, Mikrosegmentierung und Perimeter.

Der genaue Aufbau der Kundenlandschaft kann der Abbildung .5 in den Anlagen entnommen werden. Die Form der Umsetzung einer Mikrosegmentierung wird in dem nachfolgenden Kapitel beschrieben.

2.1.4 Konfiguration einer mandantenfähigen Umgebung

Nach der Bereitstellung der einzelnen Komponenten wurde eine fiktive Multimandantenumgebung erstellt. Die Kundenumgebungen wurden auf dem Compute-Cluster erstellt. In der ersten Ausbaustufe existieren zwei Kundenumgebungen, welche in Abbildung .5 in der Anlage dargestellt sind. Zum einen die „BTH“ und zum anderen sogenannte „Cus..“ Umgebungen. Die CuS-Umgebungen sind weitere kleine simulierte Mandantenumgebungen, mit welchen unterschiedliche Szenarien abgebildet werden können.

2.2 Umsetzung einer Mikrosegmentierung

Innerhalb dieser Sektion wird ein Überblick gegeben welche Werkzeuge wie eingesetzt werden können um eine „mikrosegmentierte“ Infrastruktur zu realisieren.
Für die Umsetzung einer Mikrosegmentierung stehen die logischen Firewalls der Edge Services bzw. DLR und die DFW zur Verfügung. Die Empfehlung von VMware besteht darin die logische Firewall zur Sicherung der Perimeter Grenze und die DFW zur Absicherung des internen zu nutzen. Dies bedeutet ein Regelwerk für ein- und ausgehenden Datenverkehr externer Netzwerkwerke wird an den jeweiligen Egde Services oder DLRs vorgenommen. Kommunikation innerhalb eines Netzsegmentes oder zwischen unterschiedlichen internen Netzwerken werden an der DFW konfiguriert.

Das grundlegendste an einer Mikrosegmentierung ist die Tatsache, dass jegliche Kommunikation zwischen zwei Systemen nicht vertrauenswürdig ist. Das heißt, dass im ersten Schritt eine Richtlinie in der SDDC Umgebung implementiert werden muss die jede Kommunikation unterbindet. Dies ist die Grundregel „blockiere alles“, bzw. „deny all“. In einem VMware Umfeld ist diese Regel bereits vorhanden muss jedoch in der DFW von „alles zulassen“ auf „alles blockieren“ umgestellt werden. Durch diese Maßnahme wird jeder aus- und eingehende Datenverkehr an der VM, wenn dieser nicht genehmigt worden ist, unterbunden. Dies betrifft alle Systeme an welchen die VIBs installiert worden sind. In dieser Umgebung betrifft es das EdgeRoute- und Compute-Cluster.
Aus diesem Grund sollten vor Tätigung der Änderungen, betriebsrelevante VMs, wie der vCenter Server von der DFW ausgeschlossen werden und für die Mandanten VMs ein Regelwerk erstellt werden.
Wichtiges Instrument bei der Erstellung von Richtlinien ist die Gruppierung von Elementen. In klassischen Firewallarchitekturen sind dies z.B. Zusammenfassungen von IP Bereichen. Gruppierung sind übergeordnete Objekte, welche als Kriterien für die Beurteilung in einem reglementierten Netzwerk von Datenverkehr dienen. Dabei kann es

Tabelle 2.1: Mandantenübersicht

Mandant	**Netzwerkdesign**	**Mikro-segmentierung**	**Perimeter Grenze**	**Besonderheiten**
BTH	Klassische Netzwerk-architektur, keine Tiersegmentierung	Keine Umsetzung Aller interne Verkehr ist zugelassen.	Mandanten-eigene Edge für Ausbruch.	Umgebung soll ein klassisches mittelständisches Kundennetz mit unterschiedliche Serverdiensten simulieren
CusB, CusC	Einfaches Design. zwei Netzwerk-segmente mit einem DLR als Gateway. Keine Tiereinteilung	Keine Umsetzung Aller interne Verkehr ist zugelassen.	Anbindung an die Cus-edg01 über einen DLR. Simuliert die Best Practice Variante 2.	Dienen zur Simulation der Mandanten-fähigkeit und des isolierten Datenverkehrs
CusD	Entwurf von drei Tiersegmenten. welche über einen DLR verbunden sind.	Umsetzung der Mikrosegmentierung unter der Verwendung von statischen Objekten	Anbindung an die Cus-edg01 über einen DLR. Simuliert die Best Practice Variante 2.	Alle Server des Segmentes dürfen untereinander kommunizieren. Es steh nur Server einer Abteilung in einem Tier.
CusE	Entwurf von drei Tiersegmenten, welche über einen DLR verbunden sind.	Es werden statisch und dynamische Sicherheitsgruppen verwendet um eine Mikrosegmentierung zu erreichen	Anbindung an die Cus-edg01 über einen DLR. Simuliert die Best Practice Variante 2.	Innerhalb eines Tiers stehen Server unterschiedlicher Abteilungen. Nur Server einer Abteilung dürfen untereinander kommunizieren, innerhalb sowie segmentübergreifend.
CusX, CusZ	Einfaches Design, Anbindung zweier Netzwerk-segmente an einen DLR.	Keine Umsetzung.	Jeder Mandant hat eine eigenständig Edge, welche über ein Transfernetz an die Cus-edg01 angebunden ist.	Keine eingerichtet VMs für diese Umgebungen.

sich um Kriterien von Absender und Sender oder die Art des Datenverkehrs handeln.

Bei der Betrachtung der Erstellung von Absender und Sender Gruppen ergibt sich in einer SDDC Infrastruktur der Vorteil, dass Netzwerk- und Computerkomponente aus softwaretechnischer Sicht als Objekte zur Verfügung stehen. Diese Objekte können nun verwendet werden um Richtlinien zu erstellen. Bei der Gruppierung der Objekte gibt es zwei Ansätze das dynamische oder statische Gruppieren. Von dynamischen Objekten wird gesprochen, wenn die Gruppierung flexibel anhand von gewissen Attributen abhängig ist. Ein klassisches Beispiel einer dynamischen Gruppierung ist die Einteilung anhand von Namenseigenschaften der VM. Beginnt, enthält oder endet eine VM mit einem spezifischen Teilwort wird dieser einer spezifischen Gruppe zugewiesen. Innerhalb einer VMware Umgebung stehen auch sogenannte „Security Tags“ zur Verfügung, diese können z.B. verwendet werden um VMs zu markieren die Schadsoftware enthalten. Eine Richtlinie könnte jegliche Kommunikation von VMs mit diesen „Security Tag“ blockieren sodass die Schadsoftware sich nicht mehr weiterverbreiten kann. Statische Gruppierungen entsprechen einer festen Zuordnung, wie das Nutzen eines virtuellen Switches. Es fallen ebenfalls die zuvor genannten IP-Bereichsobjekte darunter. Erhält eine VM eine IP aus einem anderen IP Bereich, greifen hierfür eventuell andere Richtlinien. Diese Richtlinien decken sich jedoch nicht mit den zugedachte Richtlinie für diese VM. Diese kann unter Umständen nicht erwünscht sein. Statische Objekte bieten zwar nicht die Flexibilität, werden jedoch häufig genutzt um einfache prinzipielle Berechtigungen zu vergeben. Als Beispiel kann hierfür die Genehmigung des Sendens eines ICMP Pakets zwischen zwei Netzwerksegmenten gestattet werden. Hierfür könnten die beiden logischen Switche der jeweiligen Netzwerksegmente ausgewählt werden und als Quelle und Ziel gesetzt werden.

Eine Kombination aus beiden Welten ist durch die Erstellung einer Sicherheitsgruppe möglich. Sicherheitsgruppen können unter dem Service Composer in VMware NSX erstellt werden. Das Menü zur Erstellung einer Sicherheitsgruppe besitzt zum einen die Möglichkeit dynamische Mitglieder zu definieren oder statische Objekte ein- oder auszuschließen. Diese Sicherheitsgruppen können als Quell- oder Zielobjekt in einer Firewallrichtlinie verwendet werden. Eine weitere positive Eigenschaft dieser Form der Gruppierung ist die Möglichkeit der Nutzung solcher Objekte innerhalb der DFW und einer Edge/DLR Firewall. Somit können diese Objekte zentral verwaltet werden und an allen Stellen eingesetzt werden.

Die Nutzung von Sicherheitsgruppen wurde in der Testumgebung mehrmals umgesetzt. Für die Gruppierung von BTH-Objekten wurden Reguläre Ausdrücke verwendet, welche aufgrund der Namensgebung prüfen ob es sich bei dem VMware Objekt um eine BTH Instanz handelt. So wurde ein regulärer Ausdruck erstellt, welcher prüft ob es sich aufgrund des VM Namens um einen BTH Client handelt: \b[BTHbth]+\–+[^CLcl].

Eine Übersicht der Optionen zur Zusammenstellung einer Sicherheitsgruppe und der

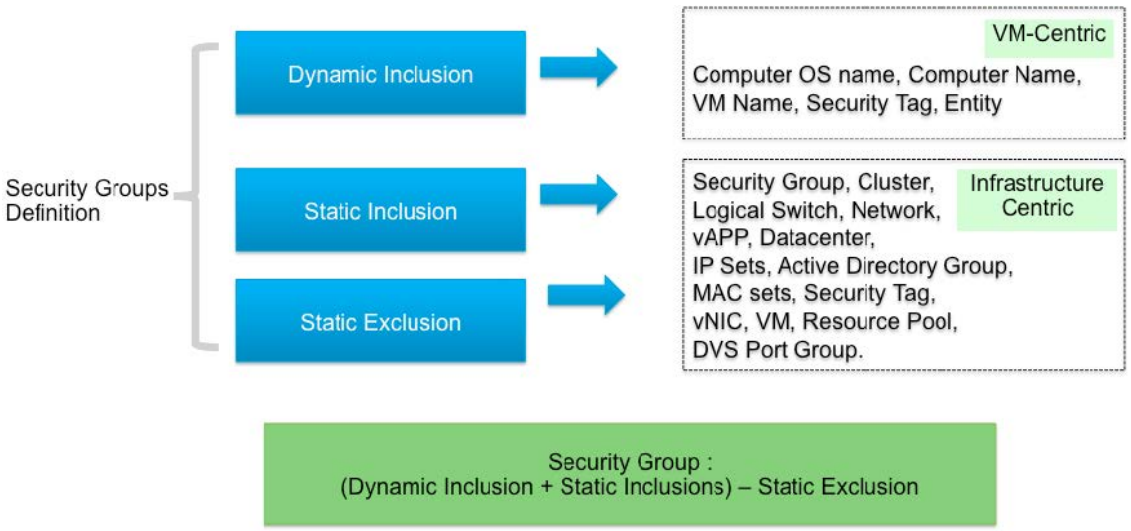

Abbildung 2.3: NSX Sicherheitsgruppendefinition, [44, S.83]

Kategorisierung der verfügbaren Elemente für eine dynamische oder statische Zuordnung kann der Abbildung 2.3 entnommen werden. Nachfolgend sollen die Vorgänge zur Umsetzung einer Mikrosegmentierung beispielhaft an den Mandanten CusD und CusE erläutert werden.

Szenario CusD:
Dieses Szenario stellt hauptsächlich den Umgang mit statischen Objekten dar. Innerhalb der drei Segmente gibt es keine zusätzlichen Beschränkungen. Dies bedeutet, dass darin befindliche Systeme mit allen Systemen in diesem Segment kommunizieren dürfen. Hierdurch können die logischen Switch Elemente zur Erstellung von Regeln verwendet werden. Als Beispiel soll nochmal das Senden eines ICMP Paketes herangezogen werden. Aufgrund der „DENY_All“ /„Blockiere alles“ Regel innerhalb der DFW ist grundsätzlich jeder Datentransfer einer VM blockiert. Durch das Erstellen einer Richtlinie „ALLOW_IntraDB_ICMP“ in welcher als Quell- und Zielobjekt der virtuelle Switch des DB-Netzwerksegmentes ist, können ICMP Pakete zwischen den beiden DB-Server ausgetauscht werden.
Bei einer segmentübergreifende Regel sind zwei Aspekte zu beachten. Zum einen muss die Regel an der DFW angelegt werden und zweitens, je nach Konfiguration, an der routenden Komponente. Standardmäßig werden diese Firewalls auf eine „DENY_ALL“ /„Alles Blockieren“ Regelung gesetzt, kann aber auch bei dem Ausrollprozess beeinflusst werden. DLRs ohne virtuelle Instanzen haben keine Firewallfunktionalität und bedürfen daher keiner Anpassung. Aus diesem Grund muss an dem Mandantenrouter cusd–dlr01 keine Änderungen vorgenommen werden. An der cus–edg01 dagegen, welche als Perimeter Firewall dient und daher den ausbrechenden Verkehr reglementiert, müssen Firewallregel konfiguriert werden. Damit der CusD Mandanten in externe Netze kommunizieren kann, bedarf es der Konfiguration der entsprechenden Richtlinien. Als Beispiel hierfür wäre der Internet Verkehr anzubringen, welcher zum einen an der DFW und zum anderen an der Edge Firewall genehmigt werden muss. [41, S.8-18]

Szenario CusE: Der Mandant CusE stellt eine Firma dar, welcher ein Netzwerksegment für Datenbankserver und eines für die Webserver besitzt. In den jeweiligen Segmenten stehen jedoch Server unterschiedlicher Abteilungen, welche nicht auf das System einer anderen Abteilung zugreifen dürfen. Bei einer solchen Form ist zu empfehlen mit Sicherheitsgruppen zu arbeiten in welcher dynamische Mitgliedschaften konfiguriert worden sind. Je Abteilung wurden zwei Sicherheitsgruppen für Systeme des Datenbank- und des Web-Segmentes erstellt. In diesem Fall wurde das Kriterium der Zuweisung in eine Sicherheitsgruppe an der Namensgebung der VM gebunden. Werden Sicherheitsgruppen genutzt, können diese auch innerhalb dieser Firewallregeln direkt konfiguriert werden. Aufgrund der Veranschaulichung wurde jedoch an dieser Stelle hiervon abgesehen. Deshalb wurde nach erfolgreichem Anlegen der Sicherheitsgruppen, innerhalb des Menüpunktes „Firewall“ die entsprechenden Firewallregel für die Kommunikation zwischen den jeweiligen Abteilungsservern der Segmente untereinander eingerichtet. Die Sicherheit der Systeme ist bei Netzwerkumstellungen wie IP Adressen oder DNS Namen Änderungen nicht betroffen. Die zuvor definierten Netzwerkrichtlinien greifen für das Serverobjekt weiterhin. [41, S.19-26]

Die oben dargestellten Testszenarien geben erstmal nur einen groben Überblick wie eine Mikrosegmentierung aussehen kann. Für eine Produktivumgebung wird es deutlich aufwendiger ein vollständiges Konstrukt an Richtlinien zu erstellen. Da an dieser Stelle mehrere Ansätze gefahren werden können:

- Flache Hierarchie
  Ein Netzwerksegment für alle Servertypen. Diese werden dann anhand von DFW Richtlinien reguliert.
- DLRs mit Firewallfunktion und mehreren Netzwerksegmenten
  Mit dieser Option werden die DFW Regularien reduziert, jedoch bedarf es dann mehreren Regeln an dem DLR, um den Datenverkehr zwischen den Segmenten zu regeln.
- DLRs ohne Firewallfunktionalität und mehreren Netzwerksegmenten DLRs werden für die Segmentierung verwendet und dadurch für das Routing, haben jedoch keine regulierende Wirkung auf den Datenverkehr. Das Regelwerk wird für den internen Datenverkehr an der DFW eingerichtet.

[41, S.64-65] Um diese Herausforderung zu stemmen, hilft eine Dokumentation der aktuellen Umgebung und eine Analyse der Regelwerke. In einer Analyse müssen dann alle reglementierende Komponenten und die Serverlandschaft betrachtet werden. Basierend auf den Ergebnissen können eventuell durch Neugestaltung der Segmente Richtlinien eingespart, bzw. Datenverkehr auch optimiert werden. Zusätzlich zu der Analyse bietet NSX die Option an Datenverkehr („Flows“) einer Umgebung mitzuschneiden und danach zu analysieren [44, S.15]. Es wird dabei von jedem hinzugefügten System der eingehende und ausgehende Datenverkehr aufgezeichnet und aufgezeigt. Wird die Aufzeichnung beendet kann mit Hilfe einer Analyse eine Auflösung des Datenverkehrs

erfolgen (Dienste, Adressen) und aus diesem Ergebnis, können direkt Firewallrichtlinien erstellt werden.

2.3 Anbindung zweier Rechenzentren mit einer L2VPN Verbindung

Unternehmen nutzen häufig Dienste die über mehrere Rechenzentren verteilt sind. Dies können von den Unternehmen oder von den Dienstanbietern geführt Rechenzentren sein. Die Gründe für die Nutzung verteilter Ressourcen können mehrere Ursachen haben. Durch die Virtualisierung und dem wachsenden Angebot von „Cloud Dienstleistungen“ sind Unternehmen auch nicht mehr in der Pflicht eigenständige Rechenzentren zu betreiben. Die Kosten für die Nutzung der „Cloud Dienste“ ist transparent und haben einen essentiellen Vorteil im Vergleich zum Aufbau einer eigenen Infrastruktur. Es muss bei der Planung kein Puffer für wachsende Anforderungen an den Systemen eingeplant werden. Wachsen die Anforderungen oder verringern sie sich, werden nur diese Leistungen gebucht und abgerechnet. [45, S.2]]

Verteilte Rechenzentren Standorte haben jedoch häufig auch einen Nachteil. So flexibel die Verwaltung von Dienst- und Systemangeboten sind, desto statischer sind die Netzwerkkonfigurationen. Zwei gängige Einsatzszenarien einer verteilten Standort Strategie sind Ausfallsicherheit und Flexibilität bei Leistungsengpässen oder Stoßzeiten neue Systeme zu installieren und diese danach abzukündigen. Diese Rechenzentren sind meistens durch VPN Verbindungen miteinander verbunden. Gerade bei der Planung einer Ausfallstrategie stehen Administratoren hier jedoch vor einer großen Herausforderung. Bei diesem klassischen Konstrukt können an beiden Standorten nur unterschiedliche IP Adresssegmente betrieben werden. Der Einsatz zweier gleichen IP Segmente ist per se nicht möglich. Dies bedeutet, es können zwar Layer 3 TCP/IP Verbindungen hergestellt werden, jedoch ist nicht einfach möglich den Layer 2 Datenverkehr zwischen zwei RZs abzubilden. Es ist hierfür eine Drittanbieterlösung notwendig. Neben der Variante von VMware‘s NSX,wäre dies beispielsweise das OTV (Overlay Transport Virtualization) von Cisco [22, S.3]. Hierbei wird technisch ein VPN Verbindung auf Basis von HTTPS zwischen zwei NSX Edges hergestellt. Innerhalb dieser Verbindung werden die gewünschten virtuelle Netze zwischen beiden Rechenzentren zur Verfügung gestellt.

Aus diesem Grund wird eine solche VPN Verbindung „Layer2 VPN“ (L2VPN) genannt. Virtuelle Netzwerke können entweder VLANs oder VXLANs sein. Dieser Vorgang wird auch als „strecken eines virtuellen Netzes“ [44, S.34] bezeichnet. Ein wichtiger Aspekt ist es die unterschiedliche virtuelle Netze miteinander verbinden zu können. Dabei müssen die VNIs nicht übereinstimmen. Die Zuordnung, ob ein VLAN mit einem VLAN oder gar VXLAN gekoppelt wird, erfolgt jeweils an der Trunk Schnittstelle. Innerhalb der VPN Verbindung hat jedes hinterlegte virtuelle Netz nochmals eine eigene Tunnel-ID an welcher die Zuordnung erfolgt. [40, S.17] Solch ein Konstrukt wird von den Anbietern und

Dienstleistern als „Hybrid-Cloud“ [45, S.3] bezeichnet. Die Bezeichnung hat sich etabliert, da für die virtuellen Systeme durch diese Technologie, gepaart mit hohen Übertragungsraten über das Internet, es aus technischer Sicht nicht mehr erkennbar ist an welchem Standort sie sich befinden. Eine zweite Eigenschaft in einer hybriden Cloud ist ein zentrales Verwaltungssystem, bzw. verknüpftes Verwaltungssystem, sodass Sicherheitseinstellungen einer virtuellen Maschine ebenfalls synchronisiert werden. Hierdurch erlangt ein Administrator zwei Vorteile. Die Administration wird vereinfacht und Wiederanlaufzeiten nach einem Ausfall verringern sich. Durch die Verwendung gleicher IP Adressbereiche, können bei einem Ausfall die gesicherten virtuellen Instanzen 1:1 hochgefahren werden und an Routing, Firewall oder Diensten müssen keine oder kaum Einstellungen vorgenommen. Ebenfalls reagieren einige Serverdienste auf IP Adressänderungen des Systems sehr empfindlich. In einem hybriden Umfeld wäre eine solche Änderung nicht mehr notwendig. [40, 45, S.3, S.13-14]

Bei der Einrichtung hybriden Cloud Umgebung gibt es zwei Phasen.
In der ersten Phase wird eine Verbindung zwischen den beiden Rechenzentren aufgebaut. Beim Aufbauen einer solcher VPN Verbindung muss an einer Edge eine Schnittstelle als „Trunk“ Schnittstelle definiert werden. Trunk Schnittstellen innerhalb eines Cisco Switching-Umfelds sind dafür bekannt, dass über solche Schnittstellen multiple VLANs übertragen werden können. Somit ist eine Trunk-Schnittstelle innerhalb des NSX mit dieser vergleichbar. [2]
Ebenfalls gilt es bei der Einrichtung zu beachten, dass eine Trunk-Schnittstelle mit einer Standard- oder verteilten Portgruppe verbunden werden muss. Diese Portgruppe muss Teil des Standard- oder verteilten Switch sein, an welchem die virtuellen Switche oder VLANs anliegen. Ist dies nicht der Fall können als „Teilschnittstellen“ nicht die dazugehörigen logischen Switche und dadurch die betreffenden VNIs ausgewählt werden. Basierend ist die VPN Verbindung auf dem Server-Client Prinzip. Das bedeutet, dass die eine Seite als VPN Server fungiert und die Gegenseite als Client. Der Verbindungsaufbau erfolgt von der Clientseite an den Server. Innerhalb des VPN Reiters der Edge wird hinterlegt ob es sich bei dieser Edge um einen Client oder Server handelt. Handelt es sich um einen Server werden die Sicherheitseinstellungen hier hinterlegt. Es können dabei Zertifikate, Benutzername und Kennwörter zur Verschlüsselung des Datenverkehrs verwendet werden. Bei den Zertifikaten kann es sich auch um selbst signierte, bzw. selbst generierte Zertifikate handeln. Der Schlüsselaustausch basiert auf dem Diffie-Hellman Verfahren und zum Erstellen der Schlüsselpaare wird das RSA (Rivest, Shamir & Adleman) Verfahren verwendet. Die Verschlüsselung der Daten erfolgt durch den AES (Advanced Encryption Standard). Hierbei kann eine Schlüssellänge zwischen 128 oder 256 Bit gewählt werden. Die Datenauthentifizierung erfolgt mittels dem SHA Algorithmus.
An einem Server können mehrere Tunnel hinterlegt werden, welchen für unterschiedliche Teilschnittstellen verantwortlich sind. Es können aber auch nur die Teilschnittstellen ausgewählt werden, welche auch zuvor an der Trunk-Schnittstelle hinzugefügt worden sind.

Der Server ist danach grundlegend konfiguriert und wartet auf eingehende Verbindungen. Auf der Gegenseite muss ebenfalls eine Trunk-Schnittstelle eingerichtet werden und die VPN-Einstellungen müssen für einen Client eingerichtet werden. [40, S.15-17]

Nach Abschluss der ersten Phase besteht eine Layer2 Konnektivität zwischen zwei logischen Netzwerken. Das bedeutet, dass virtuelle Systeme an den entsprechenden virtuellen Switchen in den Rechenzentren angebunden sind. Welche hierdurch miteinander kommunizieren können. An dieser Stelle sollte beachtet werden, dass ausbrechender Datenverkehr aus dem L2VPN befindlichen Netzen grundlegend aus dem Standardgateway ausbricht. Unter Umständen ist aber das Standardgateway in dem anderen Rechenzentrum platziert, sodass Datenverkehr erst zwischen beiden Rechenzentren übertragen werden müsste, um schließlich ins Internet zu gelangen. Um diesen Effekt zu vermeiden ist es möglich ein alternatives Standardgateway an dem VPN Server zu hinterlegen. [40, S.17] Mit Aufbau der Kommunikation ist zwar der Informationsaustausch der virtuellen Systeme möglich, jedoch müssen auch die Verwaltungssysteme miteinander verknüpft werden. Dies ist erforderlich, damit die Sicherheitsmodelle (Firewallrichtlinien, advanced security services, etc.) repliziert werden, da dies ein elementarer Bestandteil einer hybriden Cloud ist [45, S.3]. Zur Umsetzung dieser Anforderung gibt es mehrere Ansätze. In einem VMware Umfeld müssen NSX und vCenter Server miteinander verknüpft werden. Ebenfalls gibt es von VMware einen Hybrid Manager, welcher ebenfalls die Möglichkeit bietet zwei Rechenzentren miteinander zu verknüpfen und Aktionen auszuführen. Entscheidend sind aber nicht nur Anforderungen an die Software, sondern auch Anforderungen an die physische Anbindung. Möchten Dienste wie „vMotion for long distance“ genutzt werden sind nach Hersteller gewisse Latenz- und Übertragungsgeschwindigkeiten erforderlich [40, S.20].

3 Ergebnisteil

Die Grundinstallation und das Einrichten der NSX Umgebung geht vergleichsweise schnell und ist durch geführte Assistenten relativ einfach. Auch die Konfiguration erster virtueller Netzwerke können schnell mit einem positiven Ergebnis umgesetzt werden. Die Steuerung kann als Intuitiv für Mitarbeiter mit Fachkenntnis bezeichnet werden. Durch die genannten Punkte lässt sich schnell eine Umgebung aufbauen, die ein SDDC darstellt. Diese zeigt auch, dass mit in einer SDDC Umgebung das ausrollen neuer Landschaften schnell geht und ein geringerer Planungsaufwand besteht. Somit lassen sich Umgebungen für Testzwecke oder Projekte kurzfristig realisieren und durch die technische Isolation der logischen Netze, können diese mit produktiven Einstellungen betrieben werden. Hierdurch können entweder produktive Umgebungen in Testumgebungen migriert werden und für Weiterentwicklungen genutzt werden.

Für Testzwecke mag dies ein angenehmer Umstand sein, sollte jedoch für die Realisierung in einem produktiven Umfeld kein Maßstab sein. Wie schon in einzelnen Kapiteln angebracht ist eine Abstimmung der Komponenten wichtig. Die physischen Netzwerkkomponenten müssen für eine hohe Arbeitslast ausgelegt und konfiguriert sein. Als Beispiel hierfür kann der Aufbau der Transportzonen und der Behandlung des Multidestination Datenverkehr dienen. Während in einer Testumgebung eine Transportzone mit Unicast Replizierung ausreichend ist, kann dies in einer produktiven Umgebung ernsthafte Konsequenzen auf die Leistungsfähigkeit des Netzwerkes bedeuten.

Ebenfalls darf der Aufwand für eine Umstellung auf ein SDDC nicht unterschätzt werden. Da dies auch als ein „Paradigmenwechsel“ [**?**, S.17] in der Netzwerk- und Sicherheitsinfrastruktur gesehen werden kann, sind eventuell strukturelle Änderungen der bestehenden Konzepte empfehlenswert oder gar notwendig. Trotz Verschmelzung zwischen Server- und Netzwerkadministration, welche in großen Organisationen getrennt voneinander operieren, sind die Schnittstellen in einem SDDC mit einer VMware sehr groß. Administratoren welche sich zuvor ausschließlich mit Servern und derer Ressourcen auseinandersetzen mussten, können je nach Aufgabenverteilung auch die Aufgaben der logischen Netzwerkverwaltung zukommen.
Wie auch schon VMware selbst anmerkte, sind in einem SDDC weiterhin klassische Perimeter Grenzen wie Firewalls oder WAFs von entscheidender Bedeutung [36, S.28]. Diese Komponenten bieten eine Vielzahl von Sicherungsfunktionen und bewältigen diese mit einer hohen Durchsatzrate. Eine Mikrosegmentierung soll hierbei einen erweiterten Schutz bieten, sollte es einem Angreifer gelungen sein eine Perimeter Grenze zu überwältigen und sich auf Systemen einer Demilitarisierten Zone (DMZ) oder gar auf dem lokalen Netzwerk (LAN) Zutritt verschafft zu haben.

Ein weiterer Teil dieser Thesis war die Bereitstellung einer hybriden Cloud Umgebung

Diese zeigt die Vorteile einer SDN Umgebung und die technischen Möglichkeiten auf. Hybride Cloud Umgebungen sind interessante Modelle, welche IT-Entscheider neue Varianten zur Gestaltung der IT-Infrastruktur bieten. Diese Umgebungen sind eine sehr enge Verknüpfung lokaler und öffentlicher Cloudinfrastrukturen. Diese Testumgebung sollte ein mögliches Szenario mittelständischer Kunden repräsentieren. Die Umsetzung einer hybriden Cloud Umgebung konnte nicht realisiert werden. Das gewünschte Testszenario konnte aufgrund von Richtlinien des Anbieters nicht umgesetzt werden. Grundlegend wäre eine technische Umsetzung möglich gewesen, jedoch waren rechtliche Hürden vorhanden, weshalb das Szenario mit dem Anbieter nicht realisiert werden konnte.

4 Diskussion

Die in dieser Thesis entworfene Testumgebung wird in dem Diskussionsteil mit einer vergleichbaren Umgebung gegenübergestellt und analysiert. Dabei sollen infrastrukturelle Planungen sowie entworfene Sicherheitsmodelle beleuchtet und beurteilt werden. Das Konzept der Mikrosegmentierung wird hinterfragt inwieweit es eine Evolution oder gar eine Revolution für die IT-Sicherheit bedeutet. Des Weiteren wird erläutert ob ein Mehrwert durch die Umsetzung einer Mikrosegmentierung das Sicherheitsniveau erhöht.
Weitere Erkenntnisse aus den theoretischen Ansätzen und der Funktionsweise bilden die Grundlage für weiterführende Überlegungen wie sich einzelne Teilthemen aus den Bereichen des SDN und SDDC auf andere IT-Themen auswirken oder diese beeinflussen könnten.

4.1 Einordnung der Arbeit

Grundlegend handelt es sich bei dieser Thesis um eine empirische Arbeit, die die unterschiedlichen Ansichten der Technologie des Software Defined Networking zusammenfasst. Sie zeigt die Ansätze und teilweise unterschiedlichen Interpretationen einer SDN Umgebung auf. Mit Hilfe der Umsetzung einer Testumgebung mit VMware und der Implementierung von VXLAN wird dem Leser die Abstraktion veranschaulicht und schließlich die daraus resultierenden Möglichkeiten eines Overlay SDNs aufgezeigt. Die Realisierung zeigt mögliche Verwendungsszenarien für Unternehmen auf um kritische Infrastrukturen abzusichern. Ein Mittel hierzu wäre die Realisierung einer Mikrosegmentierung, oder der Layer 2 Konnektivität zwischen zwei Rechenzentren zur flexiblen Gestaltung einer Ausfallstrategie aufzubauen. Nach der Umsetzung betrachtet diese Arbeit dieser Sicherheitsniveau der Lösung und diskutiert diese.

4.2 Vergleich - Cyber Capability Development Centre (CCDC) Private Cloud Design

Paul Worth von der „IBISKA Telecom, Inc.“ entwarf für das „Defense Research and Development“ (DRDC) im Jahr 2014 ein Design für eine Private Cloud Infrastruktur basierend auf einer VMware Umgebung mit NSX. Das DRDC ist eine Dienststelle des „Department of National Defence“(DND), dem kanadischen Verteidigungsministerium. Das Ziel dieses Projektes war es eine Umgebung zu entwerfen, in welcher verschiedene Testumgebungen aufgebaut und isoliert und autark voneinander betrieben werden können. Verschiedene Teams des DRDC sollen parallel verschiedene virtuelle Umgebungen betreiben, können um aktuelle IT Bedrohungen analysieren zu können. Dabei

sollte die Umgebung flexibel, erweiterbar und effektiv für den gewünschten Nutzungszweck sein. Das Projekt wurde in drei Phasen gegliedert. Innerhalb der ersten Phase sollte die Umgebung für 5-10, in der zweiten Phase für mindestens 50 interne Benutzer ausgelegt werden. Die letzte Phase beinhaltete zu den internen Benutzern auch noch externe Benutzer, welche sich remote auf die Umgebung einwählen sollen. [38, S.6]
Der Vergleich der Umgebung bezieht sich auf die Kernelemente dieser Thesis, welche zum einen die physikalische und logische Infrastruktur, zum anderen die Sicherheit dieser Umgebung betrachtet. Dabei wird die in dieser Thesis aufgebaute Infrastruktur als „Evaluierungsumgebung“ bezeichnet.

4.2.1 Physikalische Infrastruktur

Die Umgebung des CCDC und die Evaluierungsumgebung dieser Thesis bestehen aus drei Servercluster mit jeweils zwei Knoten. Alle drei Cluster sind in beiden Umgebungen dieselben Aufgaben zugedacht. Es existiert ein Management-, Edge- und Payload-/Compute- Cluster. Die Aufgaben welchen den einzelnen Cluster zugedacht ist, stimmen in beiden Infrastrukturen überein. [38, S.17] Das Management Cluster ist für das Bereitstellen der VMware Komponenten für die Betreibung der private Cloud Struktur zuständig. Eine weitere Aufgabe ist die Verwaltung eines Protokollierungssystems. Innerhalb des CCDC wurde hierzu schon eine nähere Strategie vorgelegt, welche in der Eval-Umgebung noch nicht im Detail ausgearbeitet wurde. Während in der CCDC das Zusatzmodul, „VMware vCenter Log Insight“, zum Einsatz kommt, ist in der Eval-Umgebung keine aktive und erweiterte Protokollierung bisher implementiert. Es werden lediglich die eingebetteten Protokollierungsfunktionen genutzt. [38, S.17]
Ausbrüche in weitere Abteilungsnetze oder in das Internet werden über das Edge Cluster geleitet. Es werden hier Perimeter Schutz, Edge Services und DLRs positioniert. Über das Edge Cluster stellen Remotebenutzer den Zugriff auf die einzelnen Umgebungen her. . [38, S.39-41]
Das letzte Cluster ist das Payload Cluster und ist mit dem Compute Cluster aus der Eval Umgebung vergleichbar. Dieses Cluster enthält alle Mandanten bzw. die Testumgebungen der einzelnen Forschungsgruppen. [38, S.25] Innerhalb der physikalischen Netzwerkinfrastruktur besitzen die einzelnen Netzwerke eigenständige Broadcastdomänen, welche nach Verwendungszwecke aufgeteilt sind. Der CCDC Infrastruktur wurde noch ein zusätzliches Netzwerk hinzugefügt, in welchem die ESXi Hosts verwaltet werden. Innerhalb der Eval-Umgebung wird dies über das allgemeine Managementnetz (vCenter im CCDC tituliert) durchgeführt. [38, S.24]

Tabelle 4.1: Gegenüberstellung der VDS

Netzwerk	VDS CCDC		VDS Thesis	
HostMGMT	vSwitch0	Edge, MGMT, Payload	-	Nicht existent
vMotion	vSwitch0	Edge, MGMT, Payload	ESXvMotion	Edge, MGMT, Compute
Storage	vSwitch0	Edge, MGMT, Payload	ESXvSANlag & CC_vSAN	Edge, MGMT, Compute
vCenter/MGMT	vSwitch0	Edge, MGMT, Payload	VLAN999	Edge, MGMT, Compute
External/Uplink	vdSwitch01	Edge, Payload	NSXBreakout	Edge
Transport	vdSwitch01	Egde, Payload	NSXTransport	Egde, Compute

Unterschiede bestehen jedoch bei der Anbindung der physikalischen Netze an die ESXi Server. Zum einen ist die Umgebung des CCDC auf 10Gbit mit Fault Tolerance konfiguriert worden, was soviel bedeutet, dass Netzwerk- und Serverkomponenten redundant ausgelegt sind. Grundlegend ist dies auch in der Eval-Umgebung der Fall. Ausnahme dabei bildet der Switch für die Transportzone. Wegen der niedrigen Kritikalität der Umgebung wurden hier keine weiteren Ressourcen aufgewendet. Zur Erlangung der Redundanz stehen für zwei vSwitche vier physische Schnittstellen zur Verfügung. Dadurch teilen sich mehrere Portgruppen einen vSwitch. Innerhalb der Eval-Umgebung wurde für jedes separate Netzwerksegment ein eigenständiger VDS angelegt. Dies entspricht nur zum Teil den Empfehlungen von VMware, während für Management-, Storage-, und vMotion ein vSwitch empfohlen wird einen vSwitch anzulegen [42, S.87-S.88], wird für den NSX Bereich je Transportzone und Ausbruchsnetz je ein eigenständiger VDS empfohlen [42, S.109-110]. Die Uplink Interfaces sind in beiden Umgebungen via einem Link Aggregation Control Protocol (LACP)[3], angebunden. [38, S.20-22,25]

4.2.2 Logische Infrastruktur

Die Betrachtung der logischen Infrastruktur wird unter dem Gesichtspunkt vorgenommen, indem die virtuelle Netzinfrastruktur, aber auch die Schnittstellen zwischen den virtuellen und den physischen Netzen betrachtet werden.
Beide Umgebungen haben die Verwaltungs-, System- und Transportnetze in VLANs eingeordnet und nach obiger Zuordnung an die ESXi Server angebunden s. Tabelle 4.1.

Die CCDC Umgebung besitzt wie die obige entworfene Infrastruktur eine Transportzone, die zwischen den Clustern Payload und Edge anliegend ist. Der Datenverkehr ist in beiden Umgebungen an dem Compute/Payload Cluster VXLAN basierend und somit

[3] LACP ist eine Portbündelung zur Erhöhung der Übertragungsrate und Ausfallsicherheit

abstrahiert ist.
In beiden Infrastrukturen existiert ein eigenständiger Verzeichnisdienst, welcher die Benutzerverwaltung für die Managementumgebung übernimmt. Der Verzeichnisdient ermöglicht es Gruppen und Benutzer zu erstellen und Rechte in diesem Bereich zu definieren. So können für die Verwaltung einzelner Mandanten, Administratoren erstellt werden, welche berechtigt sind nur innerhalb des Mandanten administrative Aktivitäten durchzuführen. Sie können je nach Berechtigungsstuffe virtuelle Maschinen für die Testumgebung bereitstellen oder Protokolle überprüfen. Die Eval-Umgebung der Thesis hat ebenfalls eine eigenständige Administrationsdomäne, besetzt aber hierfür kein Benutzer- oder Gruppenmodell. [38, S.35]

4.2.3 Sicherheitsaspekte

Im nachfolgenden werden die Umgebungen des CCDC und der Thesis auf sicherheitstechnische Belange verglichen. Dabei wird beachtet wie innerhalb der jeweiligen Umgebung die Sicherheit erhöht wurde und welche Ansätze zur Erreichung dieses Ziels angegangen wurden.
Als Erstes soll der Ansatz der Absicherung des Datenverkehrs für beide Infrastrukturen betrachtet werden. Der grundlegende Ansatz den beide Umgebungen vertreten ist das Zero Trust Prinzip [38, S.14].

Jede Kommunikation zwischen den einzelnen Systemen, ob physikalisch oder virtuell, muss reglementier- und nachvollziehbar sein. Beide Umgebungen nutzen die integrierten Sicherheitsfeatures von VMware NSX. Eingesetzt werden die Edge Services zur Absicherung der Perimeter Grenze und die DFW zur Absicherung der einzelnen virtuellen Maschinen. Beide Umgebungen werden in auf Mandantenbasis betrieben [38, S.41]. Die Isolation der Mandanten basiert auf dem VXLAN Protokoll. Aufgrund der Größe der Umgebung des CCDC und der Vielzahl an Verwendungszwecken die diese Umgebung abzudecken hat wurden zusätzliche Sicherheitsmechanismen installiert. Der bereits erwähnte Verzeichnisdienst und die genutzte Automation sind Bestandteile dieser Strategie. [38, 39-40]

4.2.4 Abschlussbetrachtung

Theoretisch sind beide Infrastrukturen sehr gut zu vergleichen, da beide Umgebungen die gleichen Ziele verfolgen. Beide Landschaften wurden entworfen um Testumgebungen zu simulieren. Dabei wurden jeweils aktuelle Ansätze zur Absicherung der Infrastruktur und der bereitgestellten Mandanten gewählt. Ebenfalls kann an mehreren Stellen festgestellt werden, dass beide Umgebungen sich an die Empfehlungen des Herstellers und der staatlichen Institution hielten. Es wurde in beiden Umgebungen versuchten die IT-Landschaft nach dem Best-Practice Prinzip zu entwerfen. Staatliche Empfehlungen, wie virtualisierte Segmentierung, Segmentierung der physikalischen Infrastruktur

Tabelle 4.2: Gegenüberstellung CCDC & Eval VMware Versionen

VMware Komponenten	Version CCDC	Version Eval-Umgebung
vSphere ESXi	5.5	6.0
vSphere vCenter	5.5	6.5
NSX	6.0	6.3

und Einsatz von Firewalls konnten erfolgreich umgesetzt werden. [47, S.5-7,19]

Die Sicherheitsvorkehrungen beider Systeme zu sind gut zu vergleichen. Es wurde beide Male der Ansatz einer Mikrosegmentierung mit all Ihrer Facetten ausgewählt. Innerhalb des CCDC aufgrund der Kritikalität ein Stück weit granularer und umfangreicher. Aspekte der Automatisierung waren in der Bachelorthesis vorhanden, aber nicht in dem vollen möglichen Umfang implementiert worden wie innerhalb des CCDC. Die Automatisierung ist eine weitere Sicherheitsfunktion bewertet werden [36, S.29], da die einzelnen Betreuer der Testumgebungen nur begrenzte Rechte haben und VMs nur in Ihre Umgebung bereitstellen dürfen. Hierdurch wird verhindert, dass Unbefugte Zugang zu anderen Testumgebungen erhalten und Sicherheitslücken auftreten. [38, S.16]

Schwierigkeiten bei dem Vergleich konnte an den sehr unterschiedlichen Programmversionen der einzelnen VMware Produkte festgestellt werden. Gerade im Bereich des VMware NSX Moduls gab es mehrere Änderungen und Erweiterungen, weshalb nicht jede Funktion miteinander verglichen worden ist bzw. eine Gegenüberstellung der Funktionen durchgeführt wurde. Die Wichtigsten VMware Komponentenversionen in der Gegenüberstellung [38, S.25]:

Abschließend kann gesagt werden, dass sich beide Umgebungen sehr ähneln und viele Aspekte des SDN auf Overlay Basis beinhalten.

4.3 Hypothese - Mikrosegmentierung Revolution oder Evolution zur Absicherung kritischer Infrastrukturen

In dieser Thesis wurde der Mikrosegmentierung eine große Bedeutung beigemessen. Jedoch geht aus den bisherigen Erläuterungen nicht hervor, inwieweit die Mikrosegmentierung aktuelle Sicherheitskonzepte revolutioniert oder nur ein weitere Ergänzung ist. Diese Überlegungen sollen jetzt nachfolgend näher betrachtet werden und daraus eine Beurteilung entstehen lassen, welchen Stellenwert einer Mikrosegmentierung zukünftig zugemessen wird, bzw. werden kann.

Angreifer von Computersystemen zielen auf unterschiedliche Sicherheitslücken ab, um Zugriff auf fremde Systeme zu erlangen bzw. diese so zu beeinträchtigen das die Opfer

die Systeme nicht mehr im vollen Funktionsumfang nutzen können. Dabei gehen Angreifer wie folgt vor. Eine Infrastruktur wird auf Schwachstellen untersucht. Ist eine ausgemacht wird versucht diese zu infiltrieren. Sobald diese unter Kontrolle gebracht worden ist, werden Anstrengungen unternommen auf andere Systeme Schadprogramme oder Manipulationen bzw. Entwendung von Daten zu tätigen. Wie schon in der Einleitung beschrieben, sind hier häufig schwache bis keine Sicherheitsmechanismen installiert. Durch Verkleinerung der Netzwerksegmente und abstrahierten Datenverkehr soll diese transparenter und leichter zu überwachen sein. [39, S.20]
Um jedoch beurteilen zu können, ob es sich bei der Mikrosegmentierung um eine Evolution oder gar Revolution handelt, sollte diese unterteilt und unter mehreren Aspekten bewertet werden.

Die Idee

Datenverkehr in mehrere Segmente zu teilen ist keine neue Herangehensweise [34, S.3-5]. Da jedoch im Betreiberumfeld die Anzahl an Systemen stetig zunehmen, gelangen aktuelle Technologien zur logischen Abgrenzung von Netzwerken an Ihre Grenzen. Mit VXLAN kann diese Lücke geschlossen werden und bietet aufgrund der Adresstiefe weitere Möglichkeiten Netzwerke granularer zu trennen. Transportzonen einer VXLAN Infrastruktur können zusätzlich mit Hilfe von VLANs weiter segmentiert werden. Aufgrund dieser Möglichkeiten können noch tiefergehende Granulierungen vorgenommen werden, wodurch eine erweiterte Isolation des Datenverkehrs entsteht. Aus den oben genannten Gründen kann gesagt werden, dass die Idee durch die neuen Möglichkeiten gezielter und in einem erweiterten Rahmen eingesetzt werden kann. [33, S.5] Bei dem Prinzip des SDN Overlays nicht nur Netzwerke in Form von Adressbereiche zu Segmentierungszwecken genutzt werden sondern auch Objekte des Hypervisors Anbieters (s.h. Kapitel 1.2.4). All diese Punkte können dazu genutzt werden das Zero Trust Prinzip umzusetzen, dadurch kann die Idee und der Ansatz des Zero Trust Modells als kleine Revolution gewertet werden. Aus technologischer Sicht jedoch nicht, sondern viel mehr aus ideologischer Betrachtungswinkel der verantwortlichen Infrastrukturbetreiber. Gezielte Cyperattacken von Aktivisten und Datendiebstähle bei großen Unternehmen haben die Betreiber noch mehr sensibilisiert und die IT-Sicherheit mehr in den Fokus gerückt [23]. Wurde zuvor interner Netzwerkverkehr als weniger kritisch eingestuft, wird aufgrund der Analyse von diesen Attacken immer deutlicher, dass gezielte Angriffe auf Schwachstellen teils nicht verteidigt werden können. Es jedoch relevant ist die Architektur der Infrastruktur so zu gestalten, dass die Kommunikation innerhalb der „eigenen Mauern“ ebenfalls einer strengen Reglementierung unterliegt. [34, S.5-7]

Die Technologie

Ein weiterer Vorteil der Umsetzung des virtualisierten Datenverkehrs ist, dass dieser an virtuellen Netzwerkschnittstellen adressiert wird. Ein- oder ausgehende Datenpakete können vor jeder Seite der Schnittstelle abgefangen und inspiziert werden. Daraus ergibt sich sogar eine weitere Option, dass der Datenverkehr noch vor dem Erreichen des Systems nochmals umgeleitet werden kann. Daraufhin können noch weitere

Prüfungsmechanismen nach Schadsoftware suchen. Die Technologie ist auf bewährten Mechanismen des Tunnelings aufgebaut. Das Tunneling garantiert eine isolierte Übertragung. Dabei sollte beachtet werden, dass alle parallel betriebene Tunnel/parallele Netze über ein Kommunikationsmedium übertragen werden. Ist dieses kompromittiert und der Datenverkehr in den abstrahierten Netzen nicht verschlüsselt, so könnte dieser theoretisch mitgelesen werden. [33, S.18] Die Umsetzung auf technologischer Ebene, kann eherr als evolutionärer Schritt beurteilt werden. Es wurden bei der technologischen Realisierung keine neuen Ansätze gewählt. Die Realisierung basiert auf einem standardmäßigen Ethernet Standard (IEEE 802.3^{TM}), welcher nun mehr als 34 Jahre existiert (ausgehend von der Standardisierung) [24]. Wie in Kapitel 1.2.2 beschrieben, wird ein Ethernet Frame um zusätzliche Attribute erweitert um eine Isolation des Datenverkehrs zu erreichen. Die Implementierung von systemintegrierten und kernelbasierten Firewallfunktionalitäten auf verschiedenen Ebenen gibt Anlass dieses Konzept näher zu betrachten [47, S.19]. Der Funktionsumfang der Firewalls ist jedoch nur auf die Layer 2-4 ausgedehnt. Die Regelierung des Datenverkehrs wird zwar erreicht, ist aber für aktuelle Bedrohungen nicht mehr ausreichend [47, S.20]. Eine Erhöhung des Sicherheitsniveaus kann durch die advanced security services erreicht werden. [44, S.77]

Die Verwaltung

Zwei weitere wichtige Eigenschaften der Mikrosegmentierung sind die zentrale Verwaltbarkeit und die Automatisierung. Diese sind in der oben beschriebenen Infrastrukturen beide male gegeben. Eine zentrale Verwaltung hat den Vorteil, dass sie die Administration vereinfacht. Des Weiteren wird der Endgeräte- und Perimeter Schutz an einer zentralen Stelle administriert. Dies ermöglicht das nutzen zentral verwaltender Objekte, welche an beiden Punkten eingesetzt werden können. Im Gegensatz zu dem klassischen Modell des Endgeräteschutzes. Dies könnte z.B.: durch eine Personal Firewall realisiert werden. Der Vorteil der VMware Lösung ist es über ein zentrales Verwaltungssystem beide Systeme zu administrieren. Es bedarf keiner weiteren administrativen Oberfläche um einen Endgeräteschutz zu betreiben. (s.h. Kapitel 1.2.4)

Zusammenfassend kann davon gesprochen werden, dass das SDN eine konsequente Weiterentwicklung innerhalb des Virtualisierungsumfeld für Rechenzentren ist. Die hierdurch entstehenden Möglichkeiten, wie der Nutzung einer Mikrosegmentierung, bietet für virtuelle Systeme eine Interessanten Ansatz ein Netzwerk abzusichern. Jedoch nimmt diese Technologie nicht die Komplexität bei der Gestaltung einer Sicherheitsarchitektur für die Netzwerkinfrastruktur. Trotz zentraler Verwaltungsmöglichkeiten und der Integration von Perimeter und Endgeräteschutz sind weitere Schutzeinrichtungen notwendig. Die weiteren Schutzsysteme werden benötigt um sich vor Bedrohung $> L4$ zu schützen. Diese System verlangen weitere Produkt- und Administrationskenntnisse und bringen meist ein zusätzliche Administrationsoberfläche mit sich . Durch die Abstraktion und der Möglichkeit diverse Sicherheitsobjekte an Sicherheitsrichtlinien zu binden, kann die Komplexität noch verschärft und Unübersichtlicher werden. [44, S.151-165]

4.4 Hypothese - Hybride Umgebungen besitzen einen essentiellen Mehrwert

Ein Teil der Ausarbeitung innerhalb dieser Bachelorthesis handelt über den Aufbau einer hybriden Infrastruktur. Hybride Infrastrukturen können für zukünftige IT Landschaften immer wichtiger werden. Viele Unternehmen nutzen bereits Angebote wie z.B. Microsoft Azure Dienste in welchen Dienste wie E-Mails ausgelagert sein können [9, 14].

Ein weitere Variante einer hybriden Infrastruktur ist in Kapitel 2.3 beschrieben, in welchem eine eigene lokale und eine virtuelle Infrastruktur in einem entfernten Rechenzentrum betrieben werden. Der Unterschied zu der davor erwähnten Umgebung ist der Umstand, dass in beiden Rechenzentrumsumgebungen virtuelle Objekte selbständig installiert, konfiguriert und gewartet werden müssen. Bei der ersten Variante ist die Installation, Konfiguration und Wartungen von virtuellen Objekten, wie Servern, nur auf der lokalen Seite notwendig. Auf Seiten der öffentlichen Umgebung, werden jeweils „nur“ die gewünschten Dienste bestellt. Die Betreibung und Wartung der unterliegenden Server übernimmt der Anbieter. Der Kunde ist für die Pflege der gekauften Dienste und die korrekte Einbindung in seine eigene Infrastruktur verantwortlich. [9]

Das Modell der Buchung von Online-Diensten oder „Apps“ ist in der Praxis etabliert und erfreut sich immer weiterer Beliebtheit. Die Variante der Nutzung eines Overlay SDN hat jedoch nicht so sehr die Verbreitung gefunden, wie andere Cloudmodelle. Mit der in Kapitel 2.3 beschriebenen Variante lässt sich das Szenario zweier L2 verbundenen Rechenzentren umsetzen. Mit dem oben erwähnten Azure App Modell ist dies z.B. nicht möglich. Für die Kommunikation zwischen den Applikationen in den verschiedenen Rechenzentren werden Konnektoren benötigt, die dann intelligent die Anfragen verteilen. Dies wird von dem Anbieter auch unter dem Titel der „hybriden Cloud“ [45, S.7] vertrieben. An dieser Stelle soll diese Form nicht näher diskutiert werden. Es werden die Vorzüge des SDN in einer hybriden Cloud Umgebung analysiert und gezeigt, dass hierdurch ein essentieller Mehrwert entsteht.

Standardmäßig werden heutzutage zwei Rechenzentren mit MPLS oder VPN Verbindungen angebunden,diese auf IPSec oder HTTPS basierend sein kann. Eine L2 Konnektivität lässt sich hierdurch aber nicht umsetzen. Aktuell existieren zwei Szenarien bei welchen eine L2 Verbindung zwischen zwei Rechenzentren sinnvoll erscheint.

Bei der ersten Variante dient das Rechenzentrum A als produktiver Standort und das Rechenzentrum B als Failover. Es gilt dabei zu beachten, dass hier nicht aus Sicht eines Rechenzentrumsbetreibers dieses Szenario durchgespielt wird, sondern aus Sicht eines Kunden. Der Kunde nutzt das RZ des Rechenzentrumsbetreiber B als Notfallumgebung. Je nach Betriebsart des Clusters, „Active-Active“ oder „Active-Passive“ fallen keine oder geringe Kosten an [17, S.61-62] Bei der Form des „Active-Active Cluster“ sind alle Komponenten eines Systemverbundes aktiv und übernehmen verschiedene

Aufgaben. Die zweite Betriebsart ist die Form des „Active-Passive Clusters“ und bedeutet, dass jeweils nur eine Seite die Aktive ist. Dabei wird die andere Seite ständig aktualisiert und erst aktiv wenn der andere Knoten ausfällt. Unabhängig von der Betriebsart bedeutet es bei einem Ausfall oder einer Störung, dass die gleiche Umgebung 1 1 im gegenüberliegenden Rechenzentrum hochgefahren werden kann. Es ist unabhängig ob nur einzelne Systeme ausfallen oder ein Komplettausfall aller Systeme stattfindet. Bei einem Ausfall einzelner Systeme besteht die Möglichkeit dass der Wiederherstellungsknoten, RZ A oder RZ B, frei gewählt werden kann. [40, S.19-21]

Im zweiten Szenario gibt es ein lokales RZ A und ein RZ B, theoretisch könnten noch weitere RZs angebunden werden, sodass sich die Broadcastdomäne über mehrere RZ erstreckt. Die entfernten Rechenzentren können dazu genutzt werden Leistungsengpässe zu überbrücken oder als Ausbruchspunkte an unterschiedlichen Lokationen zu dienen. Die L2 Verbindung bildet das Rückgrat mit dem RZ A, also dem lokalen RZ, zu kommunizieren. Ausbruchsstellen vor Ort können aufgrund von Leistungsoptimierungen oder länder-/kontinentalspezifischen Gründen hinterlegt werden. Auch kann solch ein Szenario ein Ausgangspunkt für eine Migration sein wobei in den Übergangszeiten die zu migrierende Systeme in beiden oder mehreren Rechenzentren weiter betrieben werden können. [40, 17] Durch die gemeinsame, bzw. verknüpfte Verwaltungsumgebung der beiden virtuellen Infrastrukturen, können innerhalb des vCenters dieselben Sicherheitsobjekte in den verbundenen Rechenzentren verwendet werden. Dies sorgt für einen unterbrechungsfreien Schutz entweder beim Schwenken eines Clusters (Änderung des aktiven Clustersknoten) oder bei neu erstellten VMs. [44, S.31-32] Eine weitere Funktionalität innerhalb einer NSX Umgebung ist die Automatisierung. Die Automatisierung ist auch Bestandteil einer Mikrosegmentierungsstrategie. Durch die dynamische und statische Zuordnung von Sicherheitsobjekten kann eine VM sofort nach der Erstellung den Sicherheitsrichtlinien zugeordnet werden. Über die REST Schnittstelle oder weiteren Administrationsprogramme (VMware vRealize) können ganze Umgebungen (VMs, Netzwerke, etc.) über eine Oberfläche ausgerollt werden. Dabei sind die Standorte dieser Umgebungen nicht relevant. Die oben ausgeführten Punkte lassen darauf schließen, dass eine hybride Umgebung in einer SDN Umgebung nur Vorteile birken. Angefangen von einem hohen Grad an Flexibilität und Sicherheitsfunktionalitäten. [44, S.6-7]

4.5 Hypothese - Mikrosegmentierung auf NSX Basis ersetzt den Desktop Firewallansatz

Auf die integrierten Firewalls innerhalb einer NSX Umgebung ist schon mehrmals eingegangen worden. Ihre Einsatzgebiete sind der Schutz der Perimeter Grenze mit den Edge Services und der virtuellen Maschinen mit der Distributed Firewall. In der nachfolgenden Diskussion soll betrachtet werden, inwieweit die NSX DFW die im Clientbetriebssystem implementierte Personal Firewall ersetzen oder ergänzen kann. Bei der

Betrachtung sollen nur die Betriebssysteme beachtet werden, welche auch bei Unternehmen am meisten eingesetzt werden. Dies sind die Betriebssysteme von Microsoft und Linux. Des Weiteren werden keine Dritthersteller beachtet. Es werden nur die integrierten Personal Firewalls der Betriebssysteme beleuchtet.

In Linux, ab den Kernelversion 2.4, heißt das Modul zum Erstellen von Regeln zu Datenregulierung „iptables“. Dieses Modul muss standardmäßig nicht installiert sein und müsste deshalb manuell installiert werden. In der Grundinstallation findet keine Reglementierung statt. Sie ist also somit mit der DFW vergleichbar, welche nach Installation von VMware NSX standardmäßig zwar aktiviert ist, jedoch ebenfalls jeden Datenverkehr zulässt. [43, S.83]

iptables arbeitet ebenfalls auf Layer 2-4 des OSI-Schichten Modells. Es können IP-Adressen und/oder Schnittstellen als Adressobjekte und TCP oder UDP Port Nummern als zu reglementierendes Objekt ausgewählt werden.
Mit iptables lassen sich auch NAT-(Network Address Translation) Regeln und Paketmanipulationen durchführen. Es können dabei eingehende und ausgehende Pakete kontrolliert werden und an eine IP Adresse weitergeleitet werden. Iptables behandelt den Netzwerkverkehr streng nach den definierten Regeln. Trifft eine Regel zu wird das Paket gemäß dem Regelsatz definiert behandelt. Inhalte sind aber von der Überprüfung ausgeschlossen, Kriterien sind Adress- und Dienstobjekte.
In einer Unternehmensinstallation kann iptables durch zentral hinterlegte Bash-Skripte konfiguriert werden. [43, S.82-88]

Die Windows Firewall ist seit „Windows XP SP2“ und der „Windows Server 2003 SP1“ in allen Windows Installationen standardmäßig vorhanden. Sie ist standardmäßig aktiviert und auf eine „DENY_ALL “ Strategie eingestellt. Ausnahmen werden von Windows häufig von Anfang an eingetragen, wie Dateizugriffe über das Netzwerk.

Wie die DFW und iptables ist die Windows Firewall eine Layer2-4 Firewall. Es können Applikationen als Dienstobjekte hinterlegt werden. Dadurch kann für die gewählte Anwendung die Netzwerkzugriffe auf L4 Basis reguliert werden. Die Inhalte die von der Applikation übertragen wird kann die Firewall nicht kontrollieren. Die Windows Firewall überwacht und inspiziert ebenfalls eingehende und ausgehende Pakete. Durch Zuweisungen von vorgegebenen Profilen kann beeinflusst werden unter welchen Umständen eine Regel zu Tragen kommt.
Ein großer Vorteil der Windows Firewall ist die zentrale Verwaltbarkeit über die Gruppenrichtlinien des Windows Verzeichnisdienstes Active Directory. Dies gibt die Möglichkeit gleichzeitig mehrere Firewallsysteme zu konfigurieren. [48, S.18-24] Aus den obenstehenden Ausführungen wird ersichtlich, dass die DFW ohne advanced security services mit den Firewalls iptables und Windows Firewall sehr gut vergleichbar sind. Welche Ansätze zum Schutz von Endgeräte ist nun am sinnvollsten und am effektivsten? Die Fragestellung soll auf der Annahme basierend das Ziel zu haben eine Zero Trust Netz-

werkarchitektur zu realisieren. In einem ZTNA muss der Netzwerkverantwortliche immer in der Lage sein jeden Netzwerkverkehr an jeder Stelle einschränken zu können und nur gewünschte Kommunikation zu zuzulassen .

In der nachfolgenden Tabelle werden die drei Firewalls anhand von Kriterien gegenübergestellt.

Jede der genannten Firewalls hat eine Protokollierungsfunktion. Bei der Windows Firewall und den iptables werden diese lokal auf dem System abgelegt. Die DFW Logs werden auf dem ESXi Server abgelegt auf welchem die VM zu dem Zeitpunkt ausgeführt worden ist.
Wird die Tabelle 4.3 zur Beurteilung herangezogen ist es in einem VMware NSX Umgebung sinnvoll den Endgeräteschutz über die DFW zu reglementieren. Eine zentrale Verwaltungskonsole sowie eine automatisierte Funktion bieten erweiterten Schutz und können den Administrationsaufwand verringern. Jedoch muss beachtet werden, dass das Regelwerk, wenn alle Mandanten in der DFW verwaltet werden, sehr umfangreich und unübersichtlich werden kann. In gemischten Umgebungen, in welcher sowohl physische Systeme und virtuelle Systeme aktiv sind, wird zum Schutz der Endgeräte ein Mischbetrieb unumgänglich sein .

Tabelle 4.3: Gegenüberstellung DFW und Personal Firewalls Windows und Linux

Kriterium	DFW	Iptables	Windows Firewall
Verfügbarkeit	Die DFW ist nur in einem VMware NSX Umfeld vorhanden	Iptables sind unter Umständen nicht installiert und müssen über die Paketverwaltung installiert werden	Die Windows Firewall ist auf jedem Windows System (ab XP SP2) installiert.
Zeitpunkt des aktiven Schutzes	Sofort nach der Erstellung der VM. Durch Automation kann diese ein kategorisiert werden und umgehend das richtige Regelwerk erhalten. Mit den Standardeinstellungen ist jeder Verkehr gestattet.	Ist iptables installiert so ist standardmäßig jeder Verkehr gestattet.	Standardmäßig aktiviert. Windows Standardfreigaben können schon eingerichtet sein. Unternehmensrichtlinien sind erst nach Aufnahme in das Unternehmensnetzwerk möglich.
Verwaltbarkeit	Die Verwaltung erfolgt über das vCenter und ist Mandaten unabhängig.	Mit Skripten können Firewalleinstellungen verteilt werden.	Einstellung können über die Gruppenrichtlinien der Active Directory verwaltet werden.
Flexibilität	Mit Hilfe von der Automatisierung können, Regelwerke gewechselt werden, wie durch das Tagging.	Statisches Regelwerk	Statisches Regelwerk
Erweiterungen	Innerhalb der DFW ist es möglich Richtlinien aufgrund von LDAP Objekten zu erstellen. Durch die zusätzliche Funktion der advanced securtiy services, können Funktionen von Drittherstellern installiert werden.	Mit iptables können NAT Einstellungen und Paketmanipulation in der Form von Paketweiterleitung hinterlegt werden.	Über die „erweiterten Einstellungen“ können Regeln vorgegebenen Profilen zugeordnet werden und Richtlinien können Benutzer-/Gruppenbasierend greifen. Eine weitere Funktion lässt eine Verbindung nur zu, wenn diese als sicher[4] deklariert wird.

5 Fazit

Der Aufbau einer VMware NSX Umgebung ist schnell umzusetzen wenn genügend Ressourcen verfügbar sind. Die Bereitstellung einer leistungsoptimierten Umgebung erfordert erweiterte Kenntnisse. Die Herangehensweise für Erstellung einer Mandanten basierten Netzwerkinfrastruktur unterscheidet sich zu der konventionellen Weise. Die Abstraktion von Netzwerken erhöht die Komplexität und dadurch findet auch eine Beeinträchtigung der Überschaubarkeit der Gesamtumgebung statt. Um den Überblick nicht zu verlieren sollte die Funktionen der Automatisierung genutzt werden und vor allem sollte auf eine gut gestaltet und organisierte Konzeptionierungsphase wert gelegt werden. Vor der Gestaltung eines SDN muss eine intensive IST-Analyse durchgeführt werden, in welcher die Netzstruktur, die Sicherheitsorganisationen und die Teilnehmer erfasst werden. Auf Basis dieser IST-Analyse können dann weitere Planungen auf Grundlage der Grundsätze einer mikrosegmentierten IT-Infrastruktur, aufgenommen werden.

Ein SDN bietet viele Möglichkeiten und kann nicht nur zu Erhöhung der Sicherheit, sondern auch zur vereinfachten Bereitstellung von Testumgebungen. Profitieren hiervon könnten etwa Softwarehäuser, welche Testumgebung erstellen können, die identisch mit einer Produktivumgebung sind, allerdings autark voneinander arbeiten. Die Erhöhung der Sicherheit innerhalb eines SDDC kann kontrovers betrachtet werden. Die integrierten Firewallfunktionen bieten Möglichkeiten die vorher nicht und nur schwer zu tätigen waren. Jedoch ist nach heutigen Stand der Technik eine L2-L4 basierende Firewalllösung nicht mehr ausreichend. Viele Bedrohungen und Angriffe geschehen auf höher liegenden Ebenen des OSI Schichten Modells. Es kann zwar der Datenverkehr zwischen den einzelnen Systemen stark reglementiert werden, doch die erlaubten Übertragungen können nicht inspiziert werden.

An dieser Stelle kommen nun die advanced security services ins Spiel. Diese ermöglichen den Einsatz von Drittherstellerlösungen um diese Lücke zu schließen. Die Folge daraus ist, dass weitere Software, evtl. Hardware und Administrationsoberflächen installiert werden müssen. Hierdurch wächst weiterhin die Komplexität und der administrative Aufwand. Allerdings ist dies auch in konventionellen Umgebungen notwendig. IT-Sicherheit bleibt weiterhin erstmal ein modularer Baukasten, bestehend aus unterschiedlichen Sicherheits- und Analysesystemen, welche ihre eigene Komplexität mit sich bringen. Ein SDN, basierend auf einer Overlay Technologie, bietet jedoch neue Möglichkeiten in den Paketfluss einzugreifen und diesen gerade in kritischen Infrastrukturen zu beeinflussen und zu überwachen.

6 Ausblick

Abschließend soll ein Überblick gegeben werden, wo weitere Gebiete der Forschung oder der Evaluierung zu dem Themen SDN und Mikrosegmentierung liegen könnten.

Angriffsversuch auf das VXLAN Protokolls
Innerhalb des RFC werden Angriffsmöglichkeiten auf das Protokoll bzw. auf den Datenverkehr der VXLAN basierend ist, beschrieben. Hierzu können Versuchsreihen, bzw. eventuell weitere Schwachstellenanalysen betrieben werden.

Vergleich der unterschiedlichen SDN Technologien
Ein genauerer Vergleich der unterschiedlichen Interpretationen eines SDNs. Mögliche Einsatzszenarien und Beurteilung der daraus entstehenden Vorteile, bzw. Möglichkeiten. Welche SDN Lösung ist für wen die Richtige bzw. ist ein SDN nur ein Trend oder das zukünftige Netzwerkdesign

Evaluierung der Advanced Security Services in einer VMware NSX Umgebung
Hier gibt es sehr viele Ansätze, da es viele unterschiedliche Hersteller gibt, welche erweiterte Schutzmechanismen für unterschiedliche Bereiche bereitstellen. Evaluierungen können sich auf Netzwerksicherheits- oder Endgeräteschutzlösungen beschränken.

Realisierung einer Automatisierten SDN Umgebung
Entwicklung einer Anwendung/Skripte oder Nutzung von VMware Anwendungen, bzw. Drittherstellern zur Erstellung einer automatisierten SDN Umgebung. Verwendung einer alternativen Virtualisierung Plattform, z.B.: Open Stack

Hybrides Cloud Management
Evaluierung eines funktionierenden hybriden Cloud Managements zur zentralen Verwaltung. Weitere Aspekte die beachtet werden könnten, sind ISO Konformität, Betreibung von Sicherheitslösungen oder optimierte Netzwerkkommunikation in einer hybriden Umgebung.

7 Anhang

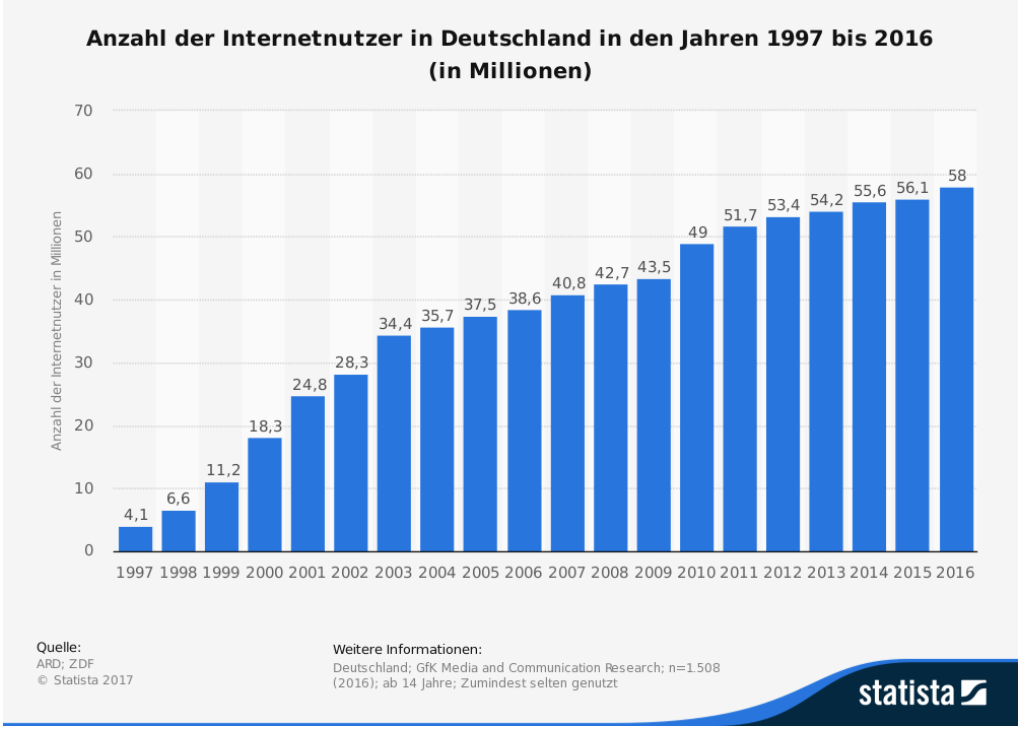

Abbildung .1: Internetnutzer in Deutschland 1997-2016, [12]

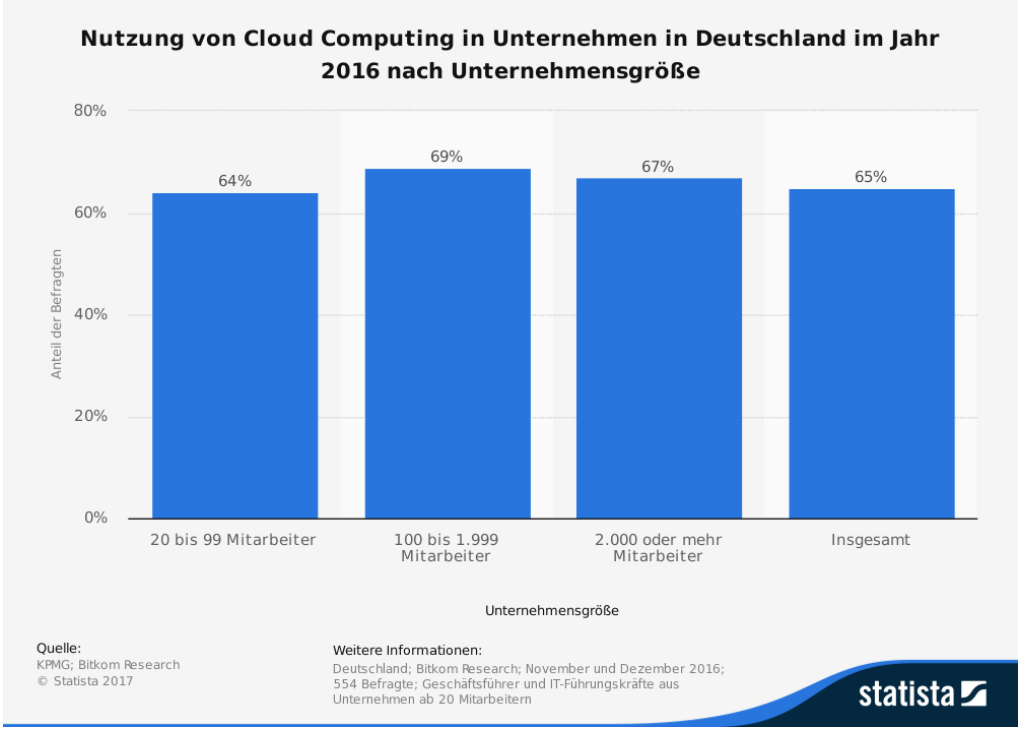

Abbildung .2: Einsatz von cloud computing in deutschen Unternehmen nach Unternehmensgroeße, [13]

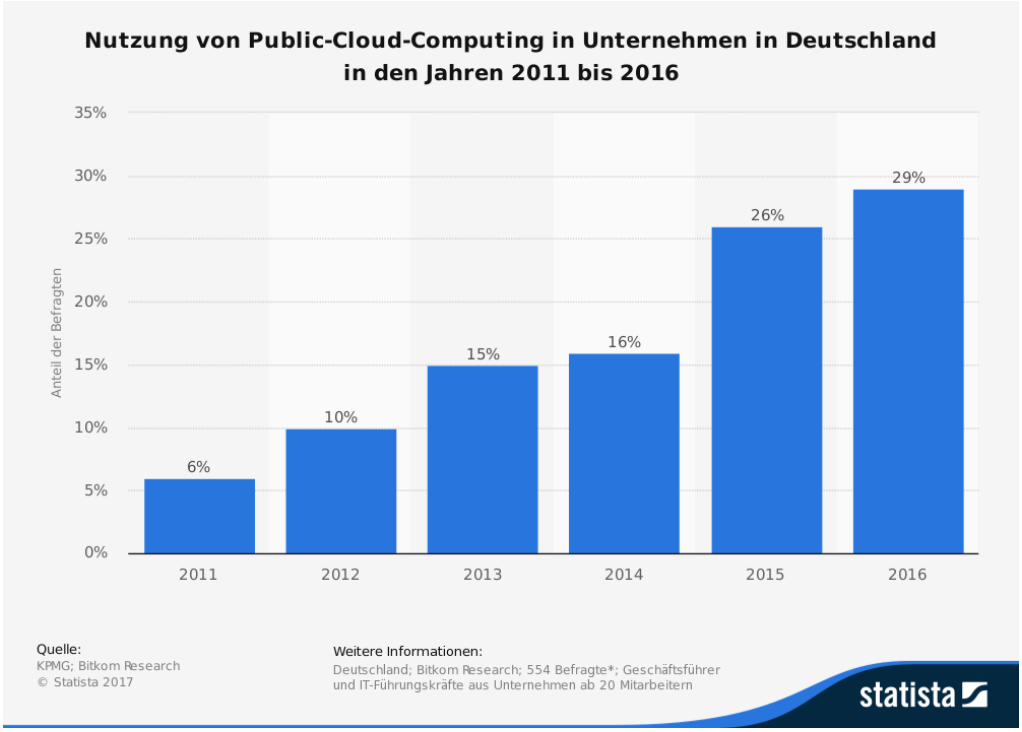

Abbildung .3: Einsatz von public cloud computing in deutschen Unternehmen 2011-2016, [14]

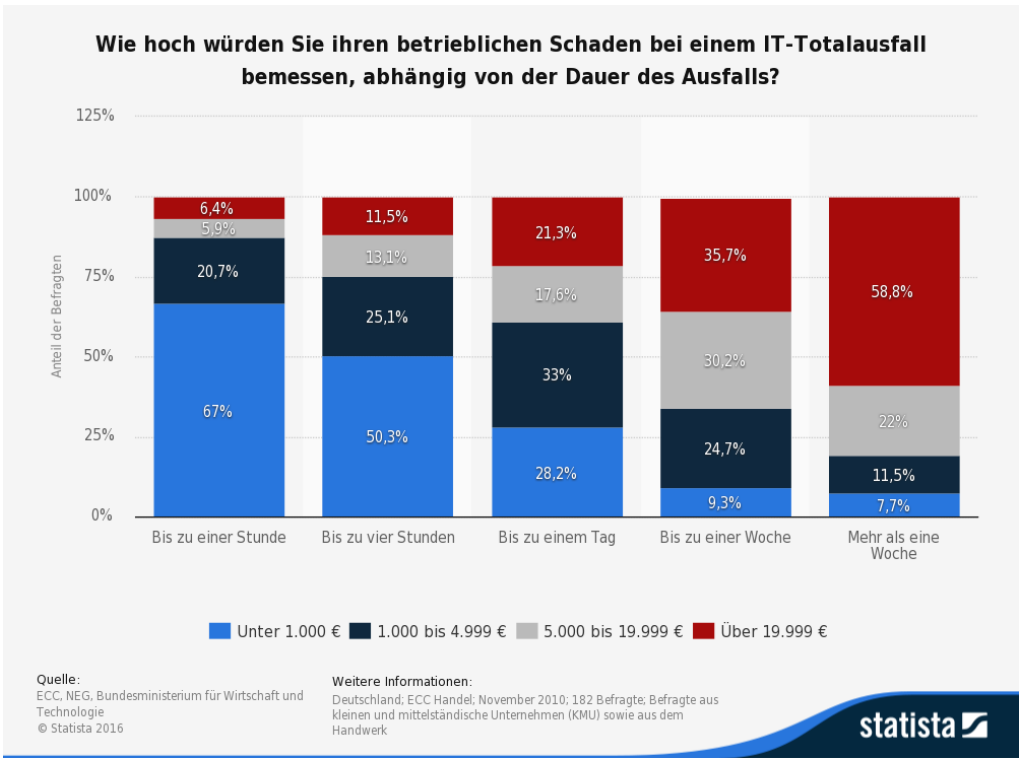

Abbildung .4: Befragung zur Schadensbemessung bei einem IT-Totalausfalls, [, STAT.04]

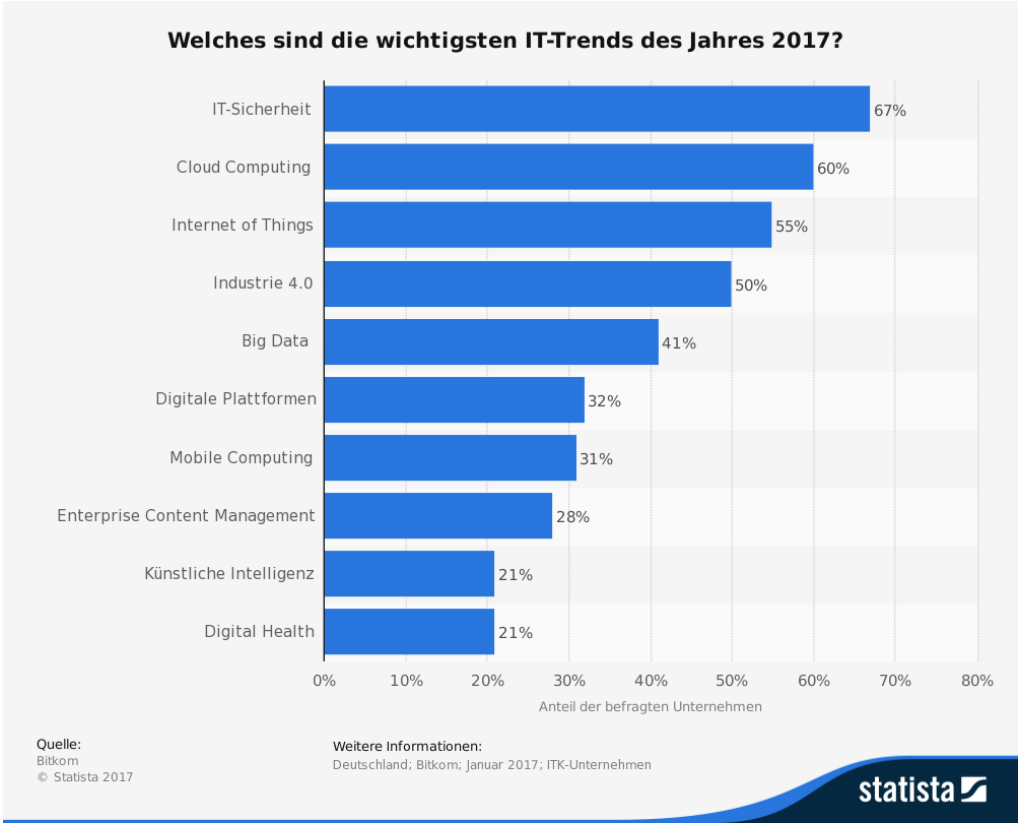

Abbildung .5: Umfrage zu den wichtigsten Trends in der ITK Branche 2017, [23]

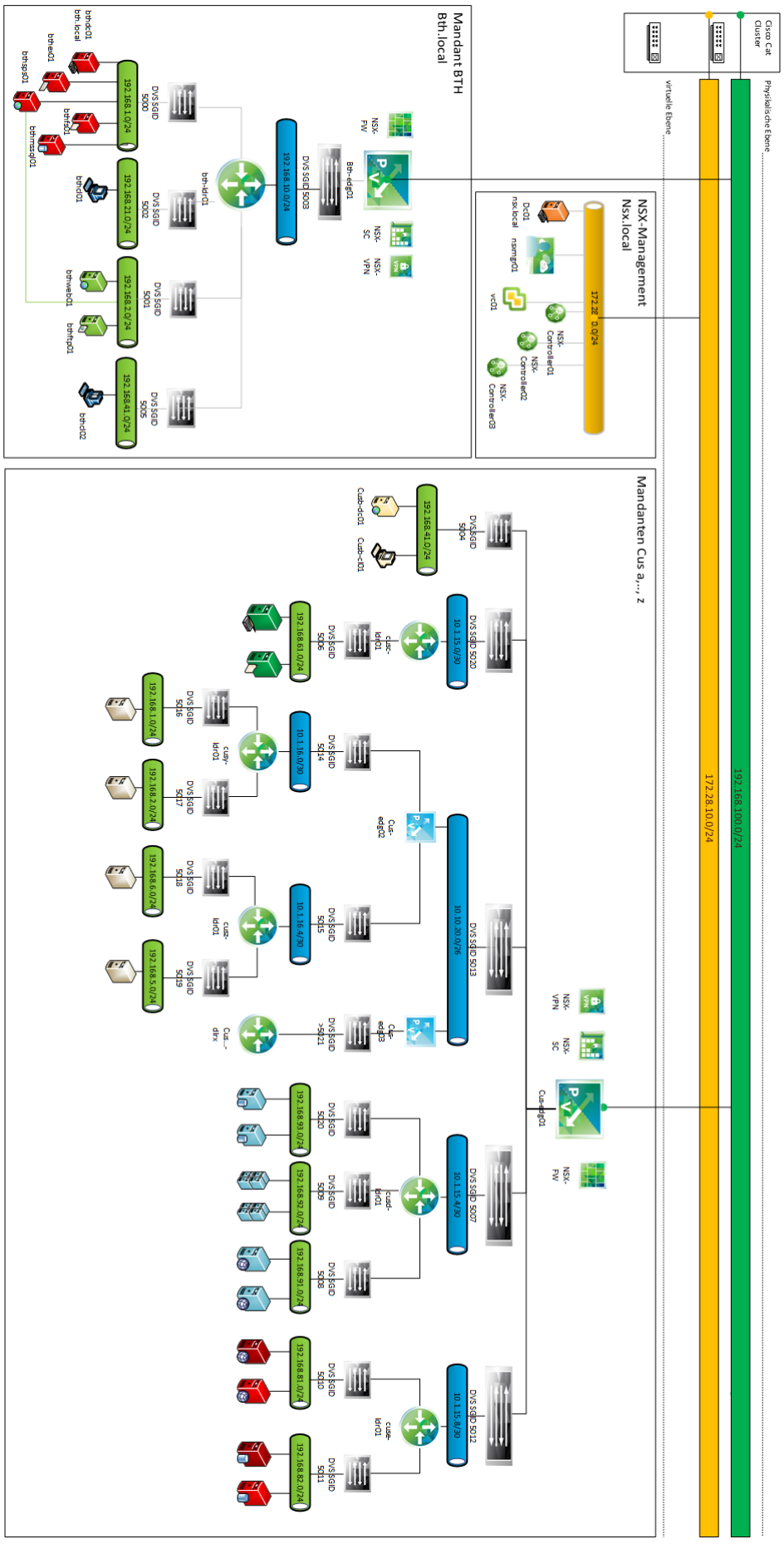

Abbildung .6: NSX Mandantenumgebung, Eigenerstellung

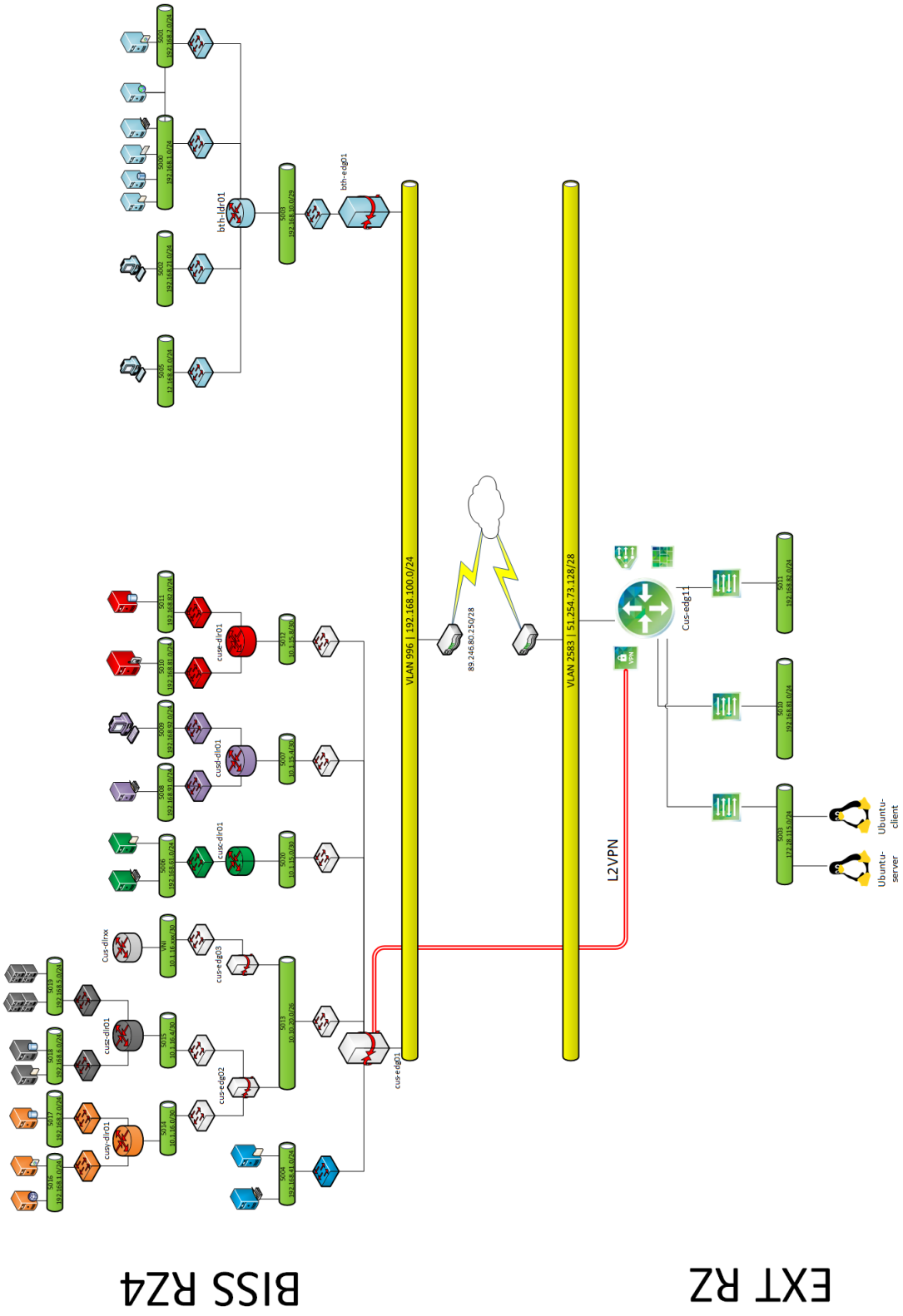

Abbildung .7: Hybride Cloudumgebung, Eigenerstellung

Literaturverzeichnis

[1] Cisco (Hg), IP Multicast Technology Overview, http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/mcst_ovr.html#wp998638, verfügbar am 21.06.2017

[2] Bertello, Giuliano, NSX for Newbies – Part 9: L2-VPN and stretched Logical Networks (on 6.1+), http://blog.bertello.org/2015/04/nsx-for-newbies-part-9-l2vpn-and-stretched-vlanvxlan-networks/, verfügbar am 07.06.2017

[3] Cisco (Hg), VXLAN Overview: Cisco Nexus 9000 Series Switches, https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/white-paper-c11-729383.html, verfügbar am 31.07.2017

[4] DATACOM Buchverlag GmbH (Hg), Netzwerkvirtualisierung :: network virtualization :: ITWissen.info, http://www.itwissen.info/Netzwerkvirtualisierung-network-virtualization.html, verfügbar am 09.06.2017

[5] RTL Television GmbH, Nach WhatsApp-Ausfall diese Woche ermittelt Forsa für "RTL Aktuell": Für knapp die Hälfte der Deutschen ist Smartphone nicht mehr aus dem Alltag wegzudenken! Forsa-Umfrage im Auftrag von RTL Aktuell, http://www.presseportal.de/pm/7847/3629126, verfügbar am 08.06.2017

[6] Kindervag, John, No More Chewy Centers: The Zero Trust Model Of Information Security, https://www.forrester.com/report/No+More+Chewy+Centers+The+Zero+Trust+Model+Of+Information+Security/-/E-RES56682, verfügbar am 07.07.2017

[7] Microsoft (Hg), Was ist IaaS? Infrastructure-as-a-Service | Microsoft Azure, https://azure.microsoft.com/de-de/overview/what-is-iaas/, verfügbar am 08.06.2017

[8] Microsoft (Hg), Was ist PaaS? Platform-as-a-Service | Microsoft Azure, https://azure.microsoft.com/de-de/overview/what-is-paas/, verfügbar am 08.06.2017

[9] Microsoft (Hg), Was ist SaaS? Software-as-a-Service | Microsoft Azure, https://azure.microsoft.com/de-de/overview/what-is-saas/, verfügbar am 08.06.2017

[10] Open Networking Foundation (Hg), Understanding the SDN Architecture - Definition -, https://www.sdxcentral.com/sdn/definitions/inside-sdn-architecture/, verfügbar am 14.06.2017

[11] Rouse, Margaret, Was ist Security Information and Event Management (SIEM)? Definition von WhatIs.com, http://www.searchsecurity.de/definition/Security-Information-and-Event-Management-SIEM, verfügbar am 31.07.2017

[12] ARD, und ZDF, Anzahl der Internetnutzer in Deutschland in den Jahren 1997 bis 2016 (in Millionen), https://de.statista.com/statistik/daten/studie/36146/umfrage/anzahl-der-internetnutzer-in-deutschland-seit-1997/, verfügbar am 06.06.2017

[13] Bitkom, "Nutzung von Cloud Computing in Unternehmen in Deutschland im Jahr 2016 nach Unternehmensgröße." Statista - Das Statistik-Portal, de.statista.com/statistik/daten/studie/305563/umfrage/einsatz-von-cloud-computing-in-deutschen-unternehmen-nach-groesse/, verfügbar am 06.06.2017

[14] Bitkom, "Nutzung von Public-Cloud-Computing in Unternehmen in Deutschland in den Jahren 2011 bis 2016." Statista - Das Statistik-Portal, de.statista.com/statistik/daten/studie/305642/umfrage/einsatz-von-public-cloud-computing-in-deutschen-unternehmen/, verfügbar am 06.06.2017

[15] NEG, und ECC Köln, "Wie hoch würden Sie ihren betrieblichen Schaden bei einem IT-Totalausfall bemessen, abhängig von der Dauer des Ausfalls?." Statista - Das Statistik-Portal, de.statista.com/statistik/daten/studie/150900/umfrage/geschaetzte-schadenshoehe-im-betrieb-bei-it-ausfall-in-deutschland/, verfügbar am 06.06.2017

[16] VMware, Inc, vSphere-Management mit vCenter Server: VMware, https://www.vmware.com/de/products/vcenter-server.html, verfügbar am 04.08.2017

[17] Epping, Duncan, vSphere 6.0 U2 HA Deepdive, v.1.1.3, https://www.gitbook.com/book/duncanyb/vsphere-ha-60-deepdive/details, verfügbar am 07.08.2017

[18] VMware, Inc, Data Center Micro-Segmentation: A Software Defined Data Center Approach for a „Zero Trust“ Security Strategy, https://blogs.vmware.com/networkvirtualization/files/2014/06/VMware-SDDC-Micro-Segmentation-White-Paper.pdf verfügbar am 29.06.2017

[19] VMware, Inc, VMware NSX Datasheet, https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-datasheet.pdf, verfügbar am 29.06.2017

[20] SDXCentral, Understanding the SDN Architecture,

https://www.sdxcentral.com/sdn/definitions/inside-sdn-architecture/, verfügbar am 01.08.2017

[21] Juniper Networks, Inc, Understanding Unknown Unicast Forwarding, https://www.juniper.net/documentation/en_US/junos/topics/concept/rate-limiting-unknown-unicast-forwarding-understanding.html, verfügbar am 15.08.2017

[22] Cisco (Hg), OTV Best Practices Configuration Guide : Configuration Guide, https://www.cisco.com/c/dam/en/us/products/collateral/switches/nexus-7000-series-switches/guide_c07-728315.pdf, verfügbar am 07.08.2017

[23] Bitkom. (n.d.). Welches sind die wichtigsten IT-Trends des Jahres 2017?. In Statista - Das Statistik-Portal, https://de.statista.com/statistik/daten/studie/675726/umfrage/die-wichtigsten-trends-in-der-itk-branche/, Zugriff am 15.08.2017

[24] Shuang Yu, IEEE 802.3™ 'STANDARD FOR ETHERNET' MARKS 30 YEARS OF INNOVATION AND GLOBAL MARKET GROWTH, http://standards.ieee.org/news/2013/802.3_30anniv.html, verfügbar am 14.08.2017

[25] Bundesministerium des Innern (Hg): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), BMI09324. Stand: 17. Juni 2009. - Berlin

[26] Chowdhury, N.M.M.K.; Boutaba, R. : Network virtualization: State of the art and research challenges. In: IEEE Communications Magazine 2009, Nr. 10.1109/MCOM.2009.5183468 S.: 20-26 - ISSN 0163-6804

[27] Hogan, Cormac; Nicholson, John: Virtual SAN 6.2 Design and Sizing Guide. - v.1.11 : VMware, Inc 2016

[28] Göransson, Paul; Black, Chuck : Software defined networks: A comprehensive approach. - 2. Aufl., ISBN 978-0-12-416675-2, Cambridge, Florida, USA: Elsevier, Inc.

[29] Gozani, Mora : Network Virtualization For Dummies®: VMware Special Edition. - Hoboken, NJ, 2016

[30] Allen, Meghan; McLachlan, Peter: NAV - Network Analysis Visualization. - Stand: 12.2004. - University of British Columbia

[31] RFC919 (v. 10.1984) Broadcasting Internet Datagrams

[32] RFC1112 (v. 08.1989) Host extensions for IP multicasting

[33] RFC7348 (v. 08.2014) Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks

[34] Kindervag, John; Balaouras, Stephanie; Coit, Lindsey: Build Security Into Your Network's DNA: The Zero Trust Network Architecture: for Security & Risk Professionals. - Cambridge : Forrester Research, Inc, 11.2010

[35] Western Mark: Developing a Framework to Improve Critical Infrastructure Cybersecurity. - Cambridge : Forrester Research, Inc, 2013

[36] Miller, Lawrence; Soto, Joshua: Micro–segmentation For Dummies®: VMware Special Edition. - 2015 -isbn 978-1-119-17734-0. - Ort: Hoboken, NJ, John Wiley & Sons, Inc.

[37] Ortiz, Sixto: Software-Defined Networking: On the Verge of a Breakthrough? In: Computer Jahrgang 2013, Nr. 7, S. 10-12, ISSN 0018-9162

[38] Worth, Paul: Cyber Capability Development Centre (CCDC) Private Cloud Design. - Stand: 11.2014 Ort: Ottawa, Department of National Defence of Canada

[39] Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland. - BSI-LB15/504. - Stand 11.2015. - Ort: Bonn

[40] Simon, Harld: Customer Onboarding with VMware NSX® L2VPN Service for VMware vCloud Air™ Network: VMware vCloud® Architecture Toolkit™ for Service Providers. - 02.2017. - v2.7. - Ort: Palo Alto, CA VMware Inc,

[41] VMware, Inc (Hg): Microsegmentation Using NSX Distributed Firewall: Getting Started: VMware NSX for vSphere, release 6.0x. - Ort: Palo Alto CA: 2014

[42] VMware, Inc: VMware Validated Design Reference Architecture Guide: VMware Validated Design for Software-Defined Data Center 2.0. - Ort: Palo Alto CA: 2016

[43] Spenneberg, Ralf: Linux-Firewalls mit iptables&Co. : Sicherheit mitKernel 2.4 und 2.6 für Linux-Server und -Netzwerke. - ISBN-13: 978-3-8273-2136-7. Stand: 2006. - Ort: München, Addison-Wesley

[44] VMware, Inc (Hg): VMware® NSX for vSphere (NSX) Network Virtualization Design Guide. - Version 3.0

[45] Mell, Peter; Grace, Timothy: The NIST Definition of Cloud Computing. - Special Publication 800-145. Stand: September 2011. - Gaithersburg: NIST

[46] VMware (Hg): Installationshandbuch für NSX : NSX for vSphere 6.3. - 2017 DE-002334-00 - Ort: Palo Alto, CA VMware Inc,

[47] Chandramouli, Ramaswamy : Secure Virtual Network Configuration for Virtual Machine (VM) Protection. - 10.6028/NIST.SP.800-125B. Stand: September 2015

[48] Vinson, Rob; Metzler Dan: Windows Firewall Applied. - Stand: März 2012

Eidesstattliche Versicherung

Hiermit versichere ich an Eides statt, dass ich meine Arbeit selbstständig verfasst, keine anderen als die angegebenen Quellen und Hilfsmittel benutzt und die Arbeit noch nicht anderweitig für Prüfungszwecke vorgelegt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Mittweida, 19. August 2017